TRANSFORMING *the* SECURITY CLASSIFICATION SYSTEM

REPORT *to the* PRESIDENT *from the*
PUBLIC INTEREST
DECLASSIFICATION BOARD

NOVEMBER 2012

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Transforming the Security Classification System	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Public Interest Declassification Board,c/o Information Security Oversight Office,700 Pennsylvania Avenue, NW Room 503,Washington,DC,20408**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**56**	

"It is time to reexamine the long-standing tension between secrecy and openness, and develop a new way of thinking about government secrecy as we move into the next century."

Report of the Commission on Protecting and Reducing Government Secrecy, 1997, Senate Document 105-2, Public Law 236

"…the only effective restraint upon Executive policy and power...may lie in an informed and enlightened citizenry - in an informed and critical public opinion which alone can here protect the values of democratic government. I should suppose that moral, political, and practical considerations would dictate that a very first principle of ...wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion."

Potter Stewart, New York Times Co. v. U.S.

Images on the following pages are courtesy of the National Archives and Records Administration, with the exception of the images on page 24 and the inside back cover which are courtesy of the National Security Agency.

TABLE OF CONTENTS

RECOMMENDATIONS *for* TRANSFORMING *the* SECURITY CLASSIFICATION SYSTEM

LETTER *to the* PRESIDENT

November 27, 2012

The Honorable Barack Obama
President of the United States
Washington, DC 20500

Dear Mr. President:

The Public Interest Declassification Board ("the Board") is pleased to submit *Transforming the Security Classification System*, the study conducted pursuant to your Implementing Memorandum (December 29, 2009) for Executive Order 13526, "Classified National Security Information." The report sets forth and explains key recommendations that flowed from the study we undertook in cooperation with the National Security Advisor to design a fundamental transformation of the security classification system.

We believe the current classification and declassification systems are outdated and incapable of dealing adequately with the large volumes of classified information generated in an era of digital communications and information systems. Overcoming entrenched practices that no longer serve the purpose of protecting our national security will prove difficult. We believe it will require a White House-led steering committee to drive reform, led by a chair that is carefully selected and appointed with specific authorities that you grant.

The Government's management of classified information must match the realities and demands in the 21st century. We hope our recommendations serve as a guide to lead the proposed committee in developing a comprehensive new policy and implementation plan.

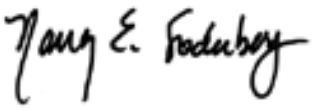
The Board has consulted extensively with experts from the Government openness advocacy community, civil society and transparency groups, archival researchers, and technologists and solicited opinions from distinguished civil servants, Executive department and agency officials, and the Congress. Our efforts were designed to gain a broad perspective on issues confronting the classification system and led to the fourteen core recommendations in this report. Sharing the recommendations with agencies has elicited a number of negative comments; there is little recognition among Government practitioners that there is a fundamental problem. Clearly, it will require a Presidential mandate to energize and direct agencies to work together to reform the classification system.

The classification system exists to protect national security, but its outdated design and implementation often hinders that mission. The system is compromised by over-classification and, not coincidentally, by increasing instances of unauthorized disclosures. This undermines the credibility of the classification system, blurs the focus on what truly requires protection, and fails to serve the public interest. Notwithstanding the best efforts of information security professionals, the current system is outmoded and unsustainable; transformation is not simply advisable but imperative.

Currently, classification and declassification do not facilitate rapid and agile information sharing required to fully support today's national security mission. It became clear to the Board that only by exploiting current and developing new technologies and applying them in an improved policy framework will the national security community be capable of managing the growing volume of electronic information created in the digital age.

If implemented, our proposed recommendations will increase efficiency, reduce costs, improve transparency and, ultimately, help restore confidence in the classification and declassification system.

Sincerely,



Nancy E. Soderberg
Chair

Executive Summary of the Report to the President from the Public Interest Declassification Board on Transforming the Security Classification System

EXECUTIVE SUMMARY

A democratic society is grounded in the informed participation of the citizenry, and their informed participation requires access to Government information. An open record of official decisions is essential to educate and inform the public and enable it to assess the policies of its elected leaders. If officials are to be accountable for their actions and decisions, secrecy must be kept to the minimum required to meet legitimate national security considerations. To maintain democratic values, Government must act to ensure openness and should have to justify any resort to secrecy. Better access to Government records and internal history will help both policymakers and the American public meet their mutual responsibilities to address national security and foreign policy challenges consistent with democratic values.

As requested by the President, the Public Interest Declassification Board (the Board) researched and studied the security classification system in cooperation with the National Security Advisor to design a fundamental transformation of the security classification system.[i] The Board sought to understand how classified records of every level of sensitivity are managed and how different users influence classification and declassification decisions at the front-end and the back-end of the system. The Board met extensively with stakeholders inside and outside of government during its study: senior government officials, Executive departments and agencies (agencies), distinguished civil servants, the Congress, leading technologists, experts from public interest, civil society and transparency groups, historians, classifiers, declassifiers, and archival researchers. Its research led the Board to understand the challenges the system presents to all users and to solicit suggestions and ideas for its transformation. The findings of the Board are conclusive; present practices for classification and declassification of national security information are outmoded, unsustainable and keep too much information from the public. The prevalence of electronic records has made the current paper-based system of classification and declassification unworkable. Use of advanced information technology is crucial to achieving increases in efficiency and better balancing information security with government openness. However, there is little evidence that Executive departments and agencies (agencies) are employing or developing the technologies needed to meet these objectives.

Reforms are essential if we expect to manage the increased volume of records, share critical information among agencies and live within available resources. Essential to such reforms must be improved integration of classification and declassification programs and better resolution of the inherent tension between keeping secrets and ensuring the openness required for an accurate historical record.

This report describes the difficulties—both technical and cultural—we face in reforming the system and recommends practicable steps to overcome them and effect reform. The Board understands the many challenges facing agencies in today's resource-constrained environment. Nonetheless, the measures in this report are critical to modernize a security classification program capable of protecting our nation and supporting fundamental democratic values and transparency. The Board recognizes there is disagreement among stakeholders with many of the recommendations in its report. Modernization is difficult and bureaucracies' natural tendency is to maintain

the status quo. These recommendations will succeed only with a determined implementation strategy and vigorous oversight backed by the President. The Board believes it will require a White House-led steering committee to drive reform, led by a chair who is carefully selected and appointed with specific authorities granted by the President. A White House-led Security Classification Reform Steering Committee, appointed by and accountable to the President, should manage the implementation of the reforms required to transform current classification and declassification guidance and practice.[ii]

Transforming the Classification System

After extensive research and discussions with stakeholders in and outside Government, the Board has concluded that the current classification system is fraught with problems. In its mission to support national security, it keeps too many secrets, and keeps them too long; it is overly complex; it obstructs desirable information sharing inside of government and with the public. There are many explanations for over-classification: most classification occurs by rote; criteria and agency guidance have not kept pace with the information explosion; and despite the Presidential order to refrain from unwarranted classification, a culture persists that defaults to the avoidance of risk rather than its proper management.

To address the concerns of excessive classification under present practice, the Board recommends:

- Classification should be simplified and rationalized by placing national security information in only two categories. This would align with the actual two-tiered practices existing throughout government, regarding security clearance investigations, physical safeguarding, and information systems domains. Top Secret would remain the Higher-Level category, retaining its current, high level of protection. All other classified information would be categorized at a Lower-Level, which would follow standards for a lower level of protection. Both categories would include compartmented and special access information, as they do today. Newly established criteria for classifying information in the two tiers would identify the needed levels of protection against disclosure of the information. Using identifiable risk as the basis for classification criteria should help in deciding if classification is warranted and, if so, at what level and duration.
- Classified national security information in the two tiered model would continue to be subject to declassification in accordance with the requirements of Executive Order 13526, "Classified National Security Information".[iii] The two tiers should be defined and distinguished by the level of identifiable protection needed to safeguard and share information appropriately, and these protection levels would determine whether classification is warranted, at what level, and for how long. Classification guidance would clearly define levels of protection by identifying a specific consequence of release of the classified information and the potential harm to the national security of limiting the sharing of the information. The difficulty of applying the current concept of presumed "damage" during derivative classification would be replaced by a more concrete application of level of protection necessary for sharing and protecting. This change in guidance would reflect how classification is actually practiced by derivative classifiers—deciding how much protection is needed based on the sensitivity of the information to both protect and share appropriately. Determining a level of protection to facilitate or impede dissemination is more prescriptive in practice and would assist classifiers in making more accurate classification decisions. Applying this risk management practice by identifying the level of protection needed based on the sensitivity of the information, rather than potential damage if disclosed, should allow users to classify information at the lowest level of protection or to keep the information unclassified. Specific protections accorded intelligence and non-intelligence sources and methods should also be better-defined and -distinguished.
- The Board recognizes that the adoption of a two-tiered model will pose greater challenges for those agencies whose internal practices are more dependent upon current distinctions between Secret and Confidential.

- Classified information that is operational or based on a specific date or event should be automatically declassified without additional review or exemption when that operation or event passes. The records containing this perishable information should be marked as classified "Short-term" (or similar term) at the time of creation.
- In order to effect the cultural shift implicit in these recommendations, guidance should assume that classification decisions are made in good faith and should afford a 'safe harbor' for classifiers who adhere to proper risk management practices and, when unsure, decide not to classify. Classification training should address the culture bias that favors classification, and often over-classification, through coordinated, consistent education that underscores the responsibility to not classify in the presence of doubt.

As discussed in the technology section of this report, available technologies, such as context accumulation, predictive analytics and artificial intelligence, should be piloted to study their effectiveness on helping implement these recommendations and to engage users and garner their trust in a new system.

Transforming the Declassification System

Declassification is a complex and time-consuming process, typically performed in a culture of caution without much attention to efficiency and risk management. Sequential referral of classified records for review by each agency that claims an "equity" in the record takes a great deal of time.[iv] Agencies are reluctant to share their declassification guidelines, impeding efficiency that could be realized from greater interagency coordination and collaboration. Because declassification is not seen as a way to serve the national security mission, the public's right to know what its government does is not well-served.

The problem is growing. Agencies are currently creating petabytes of classified information annually, which quickly outpaces the amount of information the Government has declassified in total in the previous seventeen years since Executive Order 12958 established the policy of automatic declassification for 25 year old records.[v] Without dramatic improvement in the declassification process, the rate at which classified records are being created will drive an exponential growth in the archival backlog of classified records awaiting declassification, and public access to the nation's history will deteriorate further.

To address this serious concern, the Board recommends streamlining the declassification process as follows:

- A process should be implemented for the systematic declassification review of historical Formerly Restricted Data (FRD) information. The Departments of Energy and Defense may choose to convert historical FRD information either to Restricted Data information or to classified national security information.[vi] FRD information concerns the military utilization of nuclear weapons, including storage locations and stockpile information and often dates from the end of World War II through the height of the Cold

New Classification Category	Old Classification Category	Level of Protection	
Higher-Level "Top Secret"	Top Secret	Higher level of protection	Includes compartmented and special access information
Lower-Level	Confidential and Secret	Lower level of protection	

War. Although often no longer sensitive or current, this type of FRD information is of high interest to researchers yet remains largely unavailable to the public, because there is no process for systematically reviewing it for declassification and release under the terms of the Executive Order for national security information.

- Strengthen the National Declassification Center (NDC) to establish a more coordinated government-wide declassification system.
  - Executive Order 13526 should be revised to eliminate the additional three years now authorized to process multiple agency equities in all archival records (including those outside the NDC).
  - The declassification system should manage risk and better balance resource-intensive agency reviews with the democratic value of timely public release. Rules that govern declassification, including those concerning historical nuclear information, should tolerate greater risk.[vii]
  - Streamlined archival processing should expedite public release of declassified records, with such records automatically transferred to the National Archives and Records Administration (National Archives).[viii]
  - Public representatives, including experts from the Government Openness advocacy community, should be added to the interagency NDC Advisory Panel (NAP) advising the NDC Director.[ix]
- Immediately require agencies to share declassification guidance and training and prioritize the review of historically significant records and ensure timely transfer to the National Archives.
- Streamline activities of both the NDC and agencies to complement the modernization initiatives directed by the President in his Memorandum on Managing Government Records.[x]
- Classification and declassification program staffs should collaborate with agency historians and records officers to ensure that historically significant information is identified as early as possible in its "life" and then set aside for historical review and preserved for the long-term. Agency histories, both classified and unclassified, should serve policymakers and operational leaders with "lessons learned" as well as contributing to the historical record. Agency history programs should be promoted across Government and aligned in "centers" that bring declassification reviewers and historians together. Classified histories should be reviewed at a specified interval for declassification and release to the public.
- Pilot projects should be identified to develop best practices and design a more streamlined system.

Using Technology to Aid Classification and Declassification

Classification and declassification are not keeping pace with the myriad of challenges facing the system: digital information creation, access for cleared persons, existing backlogs of paper holdings awaiting declassification review, long-term storage requirements, or the rights of a democratic society to as much information as possible about its Government. Available technologies are rarely used to meet current needs; neither are agencies preparing to use these technologies to handle the enormous volume of digital records. As a result, the Government is currently unable to preserve or provide access to a great many important records.

The challenge can be met only with determined efforts to modernize classification and declassification by employing existing technologies and developing new tools. Agencies should collaborate on policy, share technologies, promote best practices and develop common standards. Metadata are especially critical to future high-speed data manipulation in the digital era. Promising new technologies should be tested through a series of pilot projects, beginning with a declassification project at the NDC; once proven, they can be deployed at multiple agencies and then expanded to include pilot projects for classification. The ultimate goal of these pilots is to discover, develop and deploy technology that will:

- Automate and streamline classification and declassification processes, and ensure integration with electronic records management systems.

- Provide tools for preservation, search, storage, scalability, review for access, and security application.
- Address cyber security concerns, especially when integrating open source information into classified systems.
- Standardize metadata generation and tagging, creating a government-wide metadata registry. Lessons learned from the intelligence community will be helpful here.
- Accommodate complex volumes of data (e.g. email, non-structured data, and video teleconferencing information).
- Advance government-wide information management practices by supporting the President's Memorandum on Managing Government Records.

The President should hold the Steering Committee accountable for ensuring the interagency collaboration needed to employ existing technologies and develop new methods to modernize classification and declassification.

ENDNOTES *for* EXECUTIVE SUMMARY

[i] Memorandum for Implementation of the Executive Order 13526, "Classified National Security Information," December 29, 2009, 75 FR 733, Document Number E9-31424.

[ii] Modeled on the Senior Information Sharing and Safeguarding Steering Committee, Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 76 FR 63811, Document Number 2011-26729. The Public Interest Declassification Board would be available to assist this committee.

[iii] Executive Order 13526, "Classified National Security Information," 75 FR 68675, Document Number 2010-28360.

[iv] An equity is information that was originated, created by, classified by, or concerns the activities of a specific government agency or organization and, as owners of the information, only they can declassify it. Records that contain multiple agency "equities" must be referred to those agencies for declassification review. Sources: 32 C.F.R. Parts 2001 and 2003 Classified National Security Information; Final Rule, section 2001. 92(g), 75 FR 37279, Document Number 2010-15443 and The U.S. Department of Justice, Office of Information and Privacy (http://www.justice.gov/open/declassification/).

[v] One intelligence agency estimates that one terabyte of data is equivalent to approximately 112 million pages of information, making one petabyte of data equivalent to approximately 1.2 trillion pages of information. The Government declassified 1.27 billion pages of information between FY 1995 and 2011 according to figures from the FY 2011 Annual Report to the President from the Information Security Oversight Office. (*http://www.archives.gov/isoo/reports/2011-annual-report.pdf*). Executive Order 12958, "Classified National Security Information" is a predecessor order to today's Executive Order 13526. See Endnote 2.

[vi] Contemplation of recommendations regarding RD and FRD should include determination if legislative changes are needed.

[vii] Agencies have adopted conservative "no risk" practices when reviewing records for declassification. Agencies use this "no risk" practice most notably when implementing the requirements of the National Defense Authorization Acts for Fiscal Year 1999 and 2000 (Public Laws 105-261 and 106-65 respectively), which relate to RD/FRD.

[viii] Currently, many transfers of declassified records to the National Archives are hindered by outdated scheduling requirements, making declassified records unavailable to users.

[ix] The NDC Director is currently advised by an interagency NDC Advisory Panel (NAP) and assisted by an inter-agency Program Management Team (PMT). The NAP examines current declassification review processes throughout government. It consists of senior managers from the Departments of State, Defense, and Energy as well as the Central Intelligence Agency, Director of National Intelligence, the Information Security Oversight Office, and the National Archives.

[x] Managing Government Records, Memorandum for the Heads of Executive Departments and Agencies, A Presidential Document by the Executive Office of the President on 11/28/2011, 76 FR 75423, Document Number 2011-31096. The Office of Management and Budget issued *M-12-18, Managing Government Records Directive* on August 24, 2012. This Directive creates a robust records management framework that complies with statutes and regulations to achieve the benefits outlined in the Presidential Memorandum. This Directive was informed by agency reports submitted pursuant to Sec. 2 (b) of the Presidential Memorandum and feedback from consultations with agencies, interagency groups, and public stakeholders.

INTRODUCTION

"A popular Government, without popular information or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance; And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."

James Madison to W.T. Barry, August 4, 1822

A democratic society is grounded on the informed participation of the citizenry, which in turn requires access to Government information. If officials are to be accountable for their actions and decisions, secrecy must be kept to the minimum necessary to meet legitimate national security considerations. An open documentary record of official decisions is essential to educate and inform the public and enable it to assess the policies of its elected leaders. To maintain democratic values, government must act to ensure openness and should have to justify any use of secrecy.

Adequate public access to Government information by definition depends on how well government agencies record what they do and then permit access to those records. Without accurate and accessible records, history and democratic accountability suffer. Any overlay of secrecy makes accountability more difficult. At its most benign, secrecy impedes informed government decisions and an informed public; at worst, it enables corruption and malfeasance.

Technology has revolutionized the way information is created, stored, disseminated and used. This has led to an exponential increase in electronic information creation and, compared to the paper age, to vastly accelerated growth of records. For most government agencies, the information explosion of the last two decades has significantly compromised their ability to manage records properly, especially records "born digital." Policies and practices have not been modernized to keep pace with the increasing volume and changing nature of electronic records.

Modernizing records management through the use of technology will improve performance and promote openness and accountability in government. This is particularly true in the area of electronic records management. The President's recent Memorandum on Managing Government Records and its Directive specifically addresses this relationship between transparency and openness of government.[1] The memorandum calls for a much-needed modernization effort across Government to ensure improved management of records, particularly those of historical value. Among the many challenges in managing electronic records is the high cost of operating decentralized, disparate systems securely. Preserving large volumes of electronic records for future access is also problematic as media formats and retrieval hardware continually evolve.

While agencies need to modernize and improve overall records management performance, classified records pertaining to our nation's security demand particular attention. Current practices for handling classification, declassification, and management of these records are outmoded, unsustainable, and keep too much information from the public. Classification and declassification are typically performed in isolation from each other, rather than as phases in a record-keeping continuum,

and reflect an imbalance between the value of safeguarding national security information and the value of public release.

The Board previously issued a report to the White House in 2008 detailing a series of recommendations to improve the performance of the declassification system.

The report, *Improving Declassification*, led to significant changes in declassification policy.[2] Many of the Board's recommendations were included as new policy in Executive Order 13526, including the recommendation for establishing a National Declassification Center to organize and consolidate declassification efforts across Government.[3] In his Implementing Memorandum on Executive Order 13526, "Classified National Security Information," the President tasked the Public Interest Declassification Board "to design a more fundamental transformation of the security classification system," to help it function effectively and efficiently in the information age.[4]

In response to the President's tasking, the Board researched and studied the security classification system to understand how classified records of every level of sensitivity are managed and how different users influence classification and declassification decisions at the front-end and the back-end of the system. The Board met extensively with stakeholders inside and outside of government to understand the challenges the system presents to all users and to solicit suggestions and ideas for its transformation. The Board engaged senior leaders at agencies, as well as their subject matter experts, classifiers and declassifiers in their discussions. They assembled representatives from civil society and open government groups, as well as historians, researchers and information and archives professionals in academia and Government. They also consulted with leading technologists and security experts in the private sector.

The Board drafted eight preliminary recommendations based on the outcome of these meetings. As part of its outreach efforts, the Board hosted a public blog, *Transforming Classification*, launched on March 16, 2011, after a public forum held at the Newseum in Washington, D.C.[5] Subsequently, the Board expanded its recommendations into white papers and posted them for comment on the blog. To advance the online discussion, the Board solicited ideas and posted white papers submitted by the public. The blog remained active for thirteen weeks and received 104 comments. A subsequent public meeting at the National Archives invited further public participation in reviewing the draft recommendations and opened a wider dialogue about the public's white papers and comments. Discussion with key stakeholders inside and outside of government continued following the completion of the blog. The Board refined their recommendations based on these continued discussions with leaders and experts inside and outside government.

From discussion with system users, the Board learned how classification, declassification, and access-control policies come into conflict and inhibit the ability to share information critical to operations, all with great consequence to users. The Board also concluded that new policies and, likely, some new organization and culture change are necessary to transform the classification system for the digital age and better align it with public access to historical information.

Policies and practices based on an outdated secrecy bias are often counterproductive in the current information environment and require modernization. Better organizing and integrating classification, declassification, advanced technologies, and historical interests will improve access to Government records for all users. Better access to information will help our citizens and their government better manage national security and foreign policy in a complex, dangerous, and rapidly changing world.

With this background and analysis, the Board has prepared a series of recommendations on how best to transform the security classification system to protect national security more effectively while promoting government openness. Success will hinge on the Government's ability to apply new and existing technologies to advance automation and human-assisted analysis. Evaluating the effectiveness of proposed changes, particularly "piloting" new technologies prior to widespread implementation, will be critical to their acceptance in the national security community and so to their practical success in transforming the system.

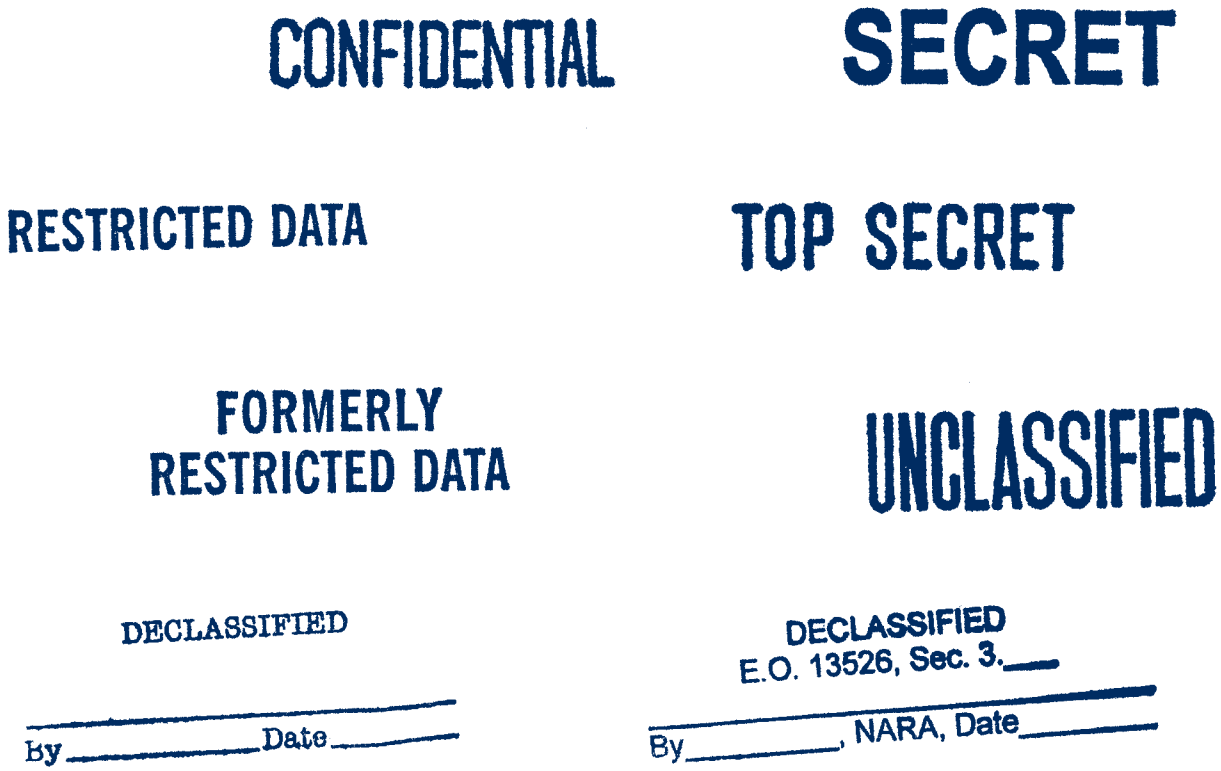
There is still much work to be done. The recommendations in this report are but a first step in a series of serious measures that can reform and modernize the security classification system. The Board recognizes that its recommendations will require discussion to address the needs of implementation. This report's recommendations are intended as a catalyst for an inter-agency process that will result in meaningful reform. Once implemented, these recommendations will ensure more open and transparent government for a society that accepts necessary, but more limited, secrecy.

THE CLASSIFICATION SYSTEM

The process for classifying information remains much as it was when first established more than 70 years ago. The methods for identifying, marking, handling and storing sensitive information have remained fairly constant. Users make decisions to assign information to one of three current categories based on loosely defined levels of presumed "damage" to national security.[6] Estimating the level of damage that might result from unauthorized release is often an exercise in speculation and more art than science, particularly when prediction of damage is inconclusive. Agencies often make these decisions in isolation, without input from other classifying agencies or knowledge of prior declassification actions. The vagaries in this process lead to imprecise and excessive classification.

From its inception, the purpose of the classification system was to categorize and protect sensitive information. Classified information lost its national security value and risked national security damage if not closely held by those who created it and their authorized customers. Historically, classification occurred mostly through a rote process, almost always favoring protection and with little restraint or concern for declassification and eventual public access. Over-classification was a natural consequence of having a culture of caution, with every incentive to avoid risk rather than manage it. Outdated and inadequate guidance and training only added to the problem, and little or no consideration was accorded to the possible tactical value of disclosure or to the public's eventual right to know.[7] As a result, limits on access were unnecessarily broad and long-lived, and the cost to store and safeguard this information dramatically increased.

The original design of the classification system was simple enough. Its rules, designations, and markings worked



fairly well to control access and prevent unauthorized disclosure of paper records. Beginning in the 1980s, an increasingly complex national security posture resulted in a sharp increase in compartmented and special access programs. These highly sensitive programs required new safeguarding, handling, and disseminating practices that were added piecemeal to a system never intended to manage such a complicated information framework. The number of cleared users increased dramatically, while the secrecy culture was compounded with more sub-categories and markings. No operational incentives existed to impose limits, and the size and complexity of the system were effectively masked from real oversight. Stove-piping not only segregated classified information, but also kept users from seeing how bloated the system had become.

A government producing substantially larger numbers of classified records in a hybrid of formats has led to a patchwork of modifications to policies and practices of the older, analog paper-based system. With the explosion of digital records, new classification guidance has developed mainly by adapting and applying outdated practices to individual cases, and so has increased the complexity of the system. This complexity makes integration and modernization more difficult and worsens over-classification.

Changes in government operations and the rapid growth of digital information reinforce the case for a new model. There is a need for more streamlined access to information by the Government and the public, challenging longstanding notions of secrecy born in the Cold War information environment. The classification system must be modernized as a dynamic, easily understood and mission-enabling system and one that deters over-classification and encourages accessibility. This will require a coordinated effort across Government beginning with an inter-agency process led by the White House.

RECOMMENDATIONS *for* TRANSFORMING CLASSIFICATION

[RECOMMENDATION 1]: *The President should appoint a White House-led Security Classification Reform Steering Committee to oversee implementation of the Board's recommendations to modernize the current system of classification and declassification.* This committee would exercise overall responsibility and ensure senior-level accountability for the coordinated interagency development and implementation of policies and standards regarding the transformation of the security classification system. The Senior Information Sharing and Safeguarding Steering Committee provides a good model for the committee. Its chair should be appointed and granted specific authorities by the President.[8] Members of the committee should be knowledgeable and experienced senior officials from the national security community, as well as officials responsible for federal information technology, records management, and public information policy and practice. It should have the authority to enact the changes recommended by the Board: identifying and implementing new initiatives, policies, and standards in support of transformation. The committee would establish, monitor, and enforce priorities and corresponding benchmarks and timeframes for meeting specific goals, reporting successes and shortcomings to the President. The Board recognizes that to be successful, the implementation process itself must be transparent and earn support from both Government agencies and the public. The Board will be available to assist the committee in carrying out the President's direction by monitoring and evaluating agency implementation efforts.

[RECOMMENDATION 2]: *Classification should be simplified and rationalized by placing national security information in only two classification categories, aligned to existing practices in much of the government.* Top Secret will remain and retain its current, high level of protection. All other classified information would be categorized at a Lower-Level (to be named), which would follow standards for a lower level of protection. Both categories would include compartmented and special access information, as they do today. The two categories should be defined and distinguished by the level of identifiable protection needed to safeguard and share information appropriately; these identifiable levels of protection would determine whether classification is warranted and at what level. The new model will require all classified information to continue to be subject to declassification and all other requirements of Executive Order 13526.

The Board's study revealed the concern by users about the increasing complexity of the classification system and accelerating growth of classified records, and confirmed a practical need to simplify policies and practices and make the system more usable. We believe that the system, in practice, need not be complex. The goal of reforming the system is to align classification levels with actual safeguarding practices throughout government. This alignment, when used in combination with accurate classification guidance linking clearly identifiable risk to classification level, will result in more precise and appropriate classification. Accurate classification most certainly aids future declassification activity, and we believe two-levels of classification may lead to less classification overall. There is a need to define more precisely and narrowly what types of information warrant security classification. The two-tiered system of classification will prod agencies to reexamine the current broad definitions of information that qualifies for classification.

The actions consequent to classifying align to only two levels of protection in Government-wide safeguarding disciplines: two levels of security clearance investigations, two levels of physical safeguarding and two levels of information systems domains. There is a practical need to simplify current policies and practices to make the system more usable. The Board found that classifying agencies in the U.S. Government and our international partners share this concern. In the case of international partners, some are moving to a two-tiered model similar to that recommended by the Board. [9] In the case of U.S. agencies, some already are operating in a de-facto two-tiered model, though the levels of classification vary (i.e.

New Classification Category	Old Classification Category	Level of Protection	
Higher-Level "Top Secret"	Top Secret	Higher level of protection	Includes compartmented and special access information
Lower-Level	Confidential and Secret	Lower level of protection	

some classify almost exclusively at the CONFIDENTIAL/SECRET levels, while for others SECRET/TOP SECRET predominate).

[RECOMMENDATION 3]: *The decision to classify information and at what level in the two-tiered system should be more clearly defined and distinguished by the level of identifiable protection needed to safeguard and share information appropriately.* The threshold for classifying in the two-tiered system should be adjusted to align the level of protection with the level of harm anticipated in the event of unauthorized release. This can only be achieved by *linking clearly identifiable risk* to an accurate harm assessment in classification guidance. Classifiers then would only be required to identify *the corresponding minimum level of protection* needed to ensure appropriate safeguarding and facilitate required information sharing. Determining a level of protection to facilitate or limit dissemination is more prescriptive in practice and would assist classifiers in making more accurate classification decisions. Applying this risk management practice by identifying the level of protection needed based on the sensitivity of the information, rather than potential damage if disclosed, would allow users to classify information at the lowest level of protection or to keep the information unclassified.

Classification guidance would need to be revised to reflect the two-tiered model, with the goals of reducing over-classification, improving authorized information sharing, and not focusing solely on the dangers of inappropriate disclosure. Guidance would clearly define levels of protection by identifying a specific consequence of release of the classified information and the potential harm to the national security of limiting the sharing of the information. The difficulty of applying the current concept of presumed "damage" during derivative classification would be replaced by a more concrete application of the level of protection necessary for sharing and protecting. This change in guidance would reflect how classification is actually practiced by derivative classifiers—deciding how much protection is needed based on the sensitivity of the information to both protect and share appropriately.

The best way to deal with over-classification and promote information sharing is to manage risk by correctly assessing potential harm and classifying to meet the minimum

CLASSIFICATION GUIDANCE UNDER THE RECOMMENDED SYSTEM WOULD ADDRESS *the specific consequences and potential harm to the national security of unauthorized release and of limitations on the sharing the information. This guidance will also provide classifiers more information at the time of classification about any likelihood the information would need to be shared with state, local, or tribal governments during a crisis. A risk management protocol would aid in deciding whether the potential harm of inadvertent release would entail more damage than the inability to share the information on a broader level and would direct classification accordingly. Currently, classification decisions are based on the loosely defined levels of presumed "damage" found in Executive Order 13526. These decisions are often made without regard to the public or tactical value of disclosure and reflect an institutional risk-averse culture that results in systematic over-classification.*

"The best way to ensure that secrecy is respected, and that the most important secrets remain secret, is for secrecy to be returned to its limited but necessary role. Secrets can be protected more effectively if secrecy is reduced overall."

Report of the Commission on Protecting and Reducing Government Secrecy, 1997, Senate Document 105-2, Public Law 236.

level of protection needed, or often even keeping the information unclassified. When considering classifying, every classifier should give serious consideration to declassification and strive to better balance the need to protect information with the public's right to access information about its government.

Confidential and Secret information in the current system require similar levels of protection against unauthorized release.[10] Classifiers are often unable to distinguish between the criteria for applying the Confidential and the Secret markings and default to the higher classification, erring on the side of protection. More difficult still is judging when to apply the criteria for the Confidential marking rather than refraining from any classification. In the simplified model, tighter definitions keyed to identifiable risks and sharper description of the protections under the new Lower-Level category should help classifiers make better decisions. The new two-tiered classification model should not simply combine the Confidential and Secret categories of classification. Although some information previously marked as Confidential may receive the Lower-Level marking in the new model, much more information should remain unclassified in the first instance. In order to simplify the system and classify less, agencies will need tighter definitions, better measures of identifiable risk and level of protection, clearer standards for access to information, and robust, new training to implement these changes.

The creation of a new Lower-Level classification category will ease the burden placed on users needing to share information that is not of the highest sensitivity. Access controls in this Lower-Level category will be the most instrumental factor in protecting information. The new

THE SIMPLIFICATION OF THE CLASSIFICATION SYSTEM TO A TWO-TIERED MODEL IS *not without meaningful challenges for agencies, particularly the Departments of State and Energy. In the FY 2011 Annual Report to the President, agencies reported to ISOO the use of Confidential in 15.2% of their total classification decisions; the State Department's use was at 27% and 61% of its original classification decisions were at the Confidential level.11 Diplomatic conversations are regularly classified as Confidential. In its meetings with senior agency officials at the State Department, the Board learned that the State Department (and many other agencies) already operates in a de facto two-tiered classification system. Currently, the State Department classifies primarily at the Confidential and Secret levels. In the new, two-tiered model the information will continue to be classified where an identifiable risk mandates a level of protection, but at the Lower-Level.*

The Department of Energy must navigate between two regimes of classification: for Classified National Security Information (under Executive Order 13526) and for nuclear information, known as Restricted Data information (under the Atomic Energy Act).12 Some Restricted Data information currently bears a Confidential marking, though its level of protection is roughly equivalent to that of Secret national security information. It will require substantial effort to harmonize and clarify the markings and protections within these two regime

PRESENTLY, THE INTELLIGENCE AND DEFENSE COMMUNITIES STRIVE FOR GREATER information sharing on their electronic networks[13] through a two-tier classification level strategy:

Network	*Category*	*Level of Protection for Classified Information*
JWICS	Top Secret/SCI	Higher level of protection compared to Secret
SIPRNET	Secret	Lower level of protection compared to Top Secret
NIPRNET	Unclassified	N/A*

**The NIPR network contains appropriate protection levels afforded controlled, unclassified information (CUI).*

Lower-Level category will enable information technology platforms to support and share classified information consistently across user domains. More unified security policy should facilitate greater system integration and improved protection. Compartmented and special access information, including Sensitive Compartmented Information, would be held, as appropriate, in either the Top Secret or the new Lower-Level category, with access tightly controlled.

[RECOMMENDATION 4]: *The specific protections afforded intelligence sources and methods need to be precisely defined and distinguished.* Intelligence sources and methods require special evaluation when determining classification. The ability to safeguard and share this type of information appropriately depends on the capacity to distinguish between intelligence and non-intelligence sources. Intelligence methods, in particular, must be more precisely defined in classification guidance to aid appropriate classification and, ultimately, declassification. The Board recognizes the compelling need to mitigate risk within this specific information grouping because of its high sensitivity.

[RECOMMENDATION 5]: *Pre-decisional, tactical, and operational information with short-lived sensitivity should be identified and segmented for automatic declassification without further review.* This type of time-specific classified information should be declassified automatically without any review *only after* the pertinent specific event occurs or date passes. It should be classified and marked as "Short-term" (or similar term) at creation, and technology should be employed to automate the declassification action. Agency declassifiers may offer expertise on the type of information that could be marked in this category. The automatic declassification of "Short-term" information would save valuable resources and inform the historical record of decisions and actions at the earliest time, hopefully earning public support and improving agency relationships with partners.

[RECOMMENDATION 6]: *Agencies should recognize in policy and practice a "safe harbor" protection for classifiers who adhere to rigorous risk management practices and determine in good faith to classify information at a lower level or not at all.* Classifiers face incentives that bias their decisions toward classification. They should be encouraged and rewarded—and at least not punished—for good-faith decisions that certain information should remain unclassified. Some agencies currently exercise these provisions and should be recognized

"Put positively, a new classification system should maintain classification for the shortest possible time and make the declassification system more efficient rather than more costly."

Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994, Joint Security Commission

IN OPERATION DESERT STORM, THE UNITED STATES LED A UN-AUTHORIZED *coalition force from 34 nations in a war against Iraq after its invasion and annexation of Kuwait. The initial action to expel Iraqi troops from Kuwait began with an aerial bombardment on January 17, 1991, followed by a ground assault on February 23. Coalition forces liberated Kuwait decisively, halted its advance into Iraqi territory, and declared a cease-fire after only 100 hours of the ground campaign.*

Command of this large-scale conflict was conducted in a mostly digital environment through the use of leadership video teleconferencing, battlefield reporting and other digital media coordination. Much of the operational and tactical military information regarding Operation Desert Storm, including records "born-digital," could have been classified and marked as "Short-term" at the time the records were created. The cease-fire declared on February 28, 1991, could have been the occasion for automatically declassifying some specific, time-limited information no longer requiring protection, including born-digital information. Such automatic declassification of born-digital information would lessen the burden of preserving this information from format obsolescence and enable study by the government and civilian historical communities at the earliest permissible time.

and serve as models of "best practice" for establishing procedures and training programs that encourage classification challenges. In addition to new policies, implementing this recommendation will depend on a fundamental change in culture and longstanding practice. Classification training should address the deep-rooted cultural bias that favors classification, and often over-classification, through coordinated, consistent education that underscores the responsibility to not classify if in doubt.

Changing the culture of classification also will require effective training in the proper use of the classification system. The Information Security Oversight Office historically has found that the quality of classification training programs varies significantly across agencies, and that many of these programs are deficient. The President should direct the Security Classification Reform Steering Committee to examine agencies' training programs and develop a strong model for training that draws on best practices.

From discussions with Executive branch officials, the Congress, and the public, the Board recognizes that over-classification impedes access to information for all users, including the public. It also undermines the integrity of the system. Agencies should be required to conduct separate training units on over-classification, which could include illustrative examples, case studies of resulting harms, an explication of the limits of the authority of derivative classifiers, and other pertinent information. This would ensure meaningful adherence to Executive Order 13526's requirement that classifiers be trained in avoiding over-classification. The Board recommends using incentives to encourage challenges to classification that would increase oversight and help shift the culture bias from favoring classification to one that recognizes the opportunity found in and need for declassification.[14]

THE DECLASSIFICATION SYSTEM

Declassification is used to remove restrictions on and grant public access to classified information that no longer requires safeguarding. The current business practices used for declassification review are slow, resource-intensive, and painstaking. In the typical review process, agency reviewers apply their own agency standards for continued classification to a document on a page-by-page, line-by-line basis. If more than one agency asserts its equities in a piece of information because of sources or origination, the document is referred for review by each agency sequentially, but with little pressure for timely action.[15] It is not a methodology designed for efficiency or for managing risk with appropriate regard for the public interest or other policy objectives.

Most agencies operate their declassification programs in isolation from each other, using disparate sets of rules and procedures. They generally do not collaborate to gain efficiency or to fashion systematic, government-wide approaches to declassification. Because agencies' declassification guidelines and criteria are often outdated or difficult to understand, they can produce inconsistent declassification decisions and missed referrals to other agencies. Agencies rarely share internal classification and declassification guidance, fearing loss of control of their information equities and contributing to partner agencies' lack of understanding of their specific interests and sensitivities. This sort of disjointed approach may put classified information needlessly at risk while also avoiding timely declassification of information.

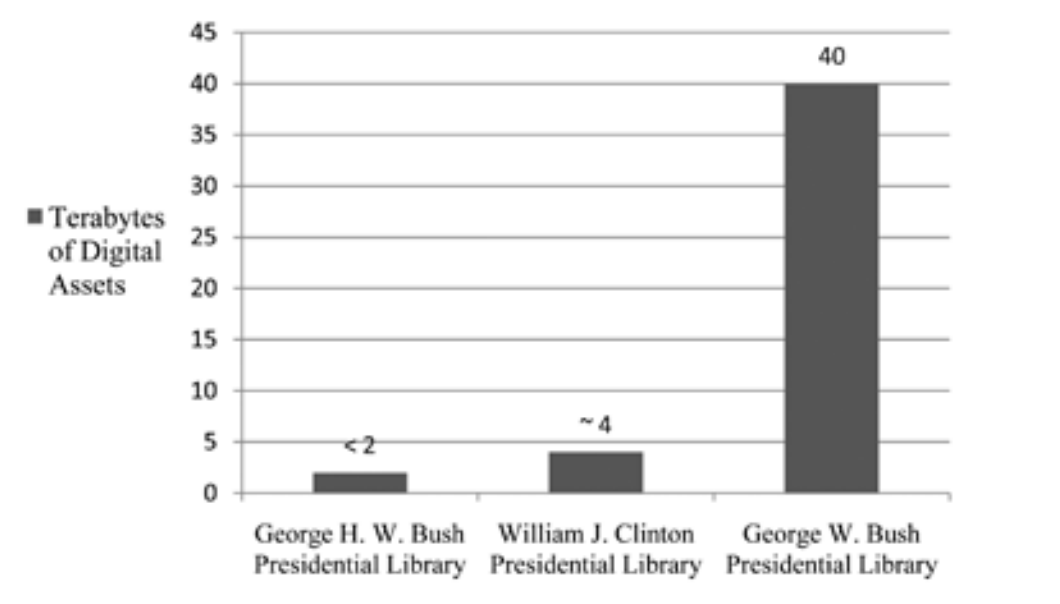
Today's national security actions increasingly produce records containing information from several agencies. The current process of referring records between agencies to complete declassification review may take years to coordinate and complete. The slow pace of declassification can also be traced in part to inadequate declassification training and outdated or confusing guidance.

Desktop computers and email changed the landscape of Government operations. "Information" is produced and shared easily, and data volumes have soared. The current approach to declassification, rooted in the paper-based past, is comprised of multiple layers of human review, lacking both a risk management approach and the advantages of modern technology. It is clear that current capabilities and business practices will never be up to the task of handling the volume of digital records held by, and being newly created across, Government. Without changes, the exponential growth in the creation of digital records requiring review will radically increase backlogs, and thus dramatic reform of the review process is needed.

Beyond the sheer volume, classified data exist in varying technical formats and are subject to decentralized agency-centric management and policies. Government has failed so far to manage review of the paper records and media created in the 20th century. Agencies are not using available technologies fully or consistently, although this would surely improve efficiency and effectiveness. The demands presented by 21st century digital data generation underscore the need to replace the traditional, time-intensive, agency declassification process with an integrated Government-wide system that takes advantage of today's digital age technologies.

Executive Order 13526, "Classified National Security Information" and its two predecessors established specific declassification requirements for all national security agencies.[20] Despite these identical mandates, a Government-wide approach to declassification remains elusive. Separate agency declassification programs evolved into a segmented declassification system where each agency reviewed its information and attempted to identify any classified information from other agencies. Agencies were

A SNAPSHOT OF THE LOOMING DIGITAL CHALLENGE



This graph represents one isolated example of just how quickly the volume of digital information assets is growing at agencies across Government.[16] According to the National Archives' estimates, the Presidential Libraries alone hold the equivalent of at least 5 billion pages of digital information in need of review.[17] Lining the pages end-to-end would stretch over 631,313 miles and would be long enough to circle the Earth more than 25 times. Even as we struggle to comprehend numbers of this size, agencies are predicting further exponential information growth at shorter intervals.

required to perform the same tasks, such as completing automatic, systematic, and mandatory declassification reviews, yet how agencies designed and implemented their specific programming to meet requirements was conducted without interagency coordination. The declassification system has become increasingly complex and unwieldy. Accordingly, the public has become increasingly frustrated and confused by what it encounters when trying to navigate the labyrinth of agency programs.

Executive Order 13526 also mandates that all classified information be automatically declassified by agencies when it is 25 years old. The birth date of records soon subject to automatic declassification coincides with the dawn of the digital Internet Age: classified records from 1988 will be automatically declassified on January 1, 2013. Agencies are unprepared and ill-equipped to handle the difficult task of reviewing the enormous volume of these so-called "born-digital" records as they become

AT ONE INTELLIGENCE AGENCY ALONE, IT IS ESTIMATED THAT APPROXIMATELY 1 *petabyte of classified records data accumulates every 18 months. One petabyte of information is equivalent to approximately 20 million four-drawer filing cabinets filled with text, or about 13.3 years of High- Definition video.[18]*

*Under the current declassification model, it is estimated that one full-time employee can review **10 four-drawer filing cabinets of text records in one year**. In the above example, it is estimated that one intelligence agency would, therefore, require **two million employees** to review manually its one petabyte of information each year. Similarly, other agencies would hypothetically require millions more employees just to conduct their reviews.*

FILE FORMAT OBSOLESCENCE: *The Threat to Long-term Maintenance of Digital Assets*[19]

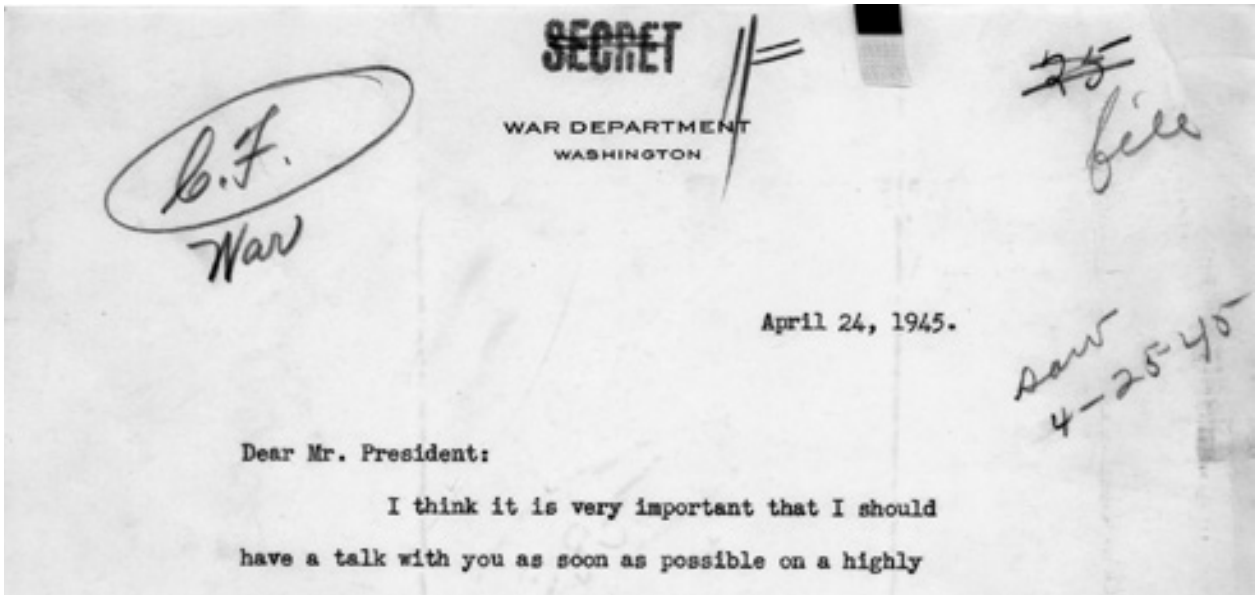
During the early decades of computing, no systematic efforts were made to collect software documentation or file format specifications. Without proper documentation, the task of trying to interpret an old file, or even determine what format it was written in, becomes daunting.

Case in Point: While we may not have realized the threat of obsolescence when we first started purchasing personal computers over twenty years ago, we certainly experience the frustration of it now. Trying to read an old 3.5 floppy from ten years ago can be frustrating if you don't know what software or hardware was involved in its creation. Say you find a ten year old PC to test an old floppy on and it is unable to read it. You may believe the floppy is damaged, but it could just as easily be an old Macintosh floppy, which your PC would be unable to identify because it runs a different Operating System. Most people would probably throw that floppy in the bin, unaware that those files were just fine.

subject to automatic declassification after 25 years. In 2009, the Board noted that "future historians may find that the paper records of early American history provide a more reliable historical account than the inchoate mass of digital communications of the current era."[21] This concern persists today, and has only grown worse.

The automatic declassification efforts begun during the Clinton Administration to improve transparency and access to information have been hamstrung by the complex and inefficient interagency referral and review processes. This has resulted in a processing backlog at the National Archives of approximately 400 million pages older than 25 years. In an effort to address the growing backlog, the President established the National Declassification Center (NDC) within the National Archives to "streamline declassification processes, facilitate quality-assurance measures, and implement standardized training to allow more effective and efficient declassification review of records determined to have permanent historical value."[22]

In addition to records awaiting standard declassification review, the backlog includes records pending review for other access restrictions, such as proper handling of historical nuclear information, Privacy Act compliance, and archival records processing. [23] These are additional, resource-intensive procedures that must be completed by agencies, the NDC, and the National Archives before records are made available to the public. The President instructed agencies to develop more cooperative processes


SECRET

WAR DEPARTMENT
WASHINGTON

25
file

b.f.
War

April 24, 1945.

Dan
4-25-45

Dear Mr. President:

I think it is very important that I should have a talk with you as soon as possible on a highly

THE 9/11 COMMISSION REPORT CITED THE NEED FOR INCREASED INFORMATION *sharing across agencies and with Government partners to better protect national security interests.26 Success in combating the nation's adversaries may dictate refraining from classification or downgrading or declassifying information to permit access. Despite this imperative, declassification continues to be conducted largely in isolation as before, despite the need for greater collaboration and better access to information*

to eliminate this backlog and make as many records accessible to the public as possible by the end of 2013.[24] Although the NDC has streamlined declassification review and has sizably reduced the backlog, its bi-annual reports indicate that it may not meet the President's prescribed goal to eliminate the backlog. [25] The expected growth of electronic records will create new backlogs almost incomprehensible in size.

Under the terms of Executive Order 13526, agencies may exempt from declassification specific information as it becomes 25 years old if release would damage national security. Guided almost exclusively by the need to identify records requiring continued protection, agencies have followed page-by-page review practices with little or no attempt to prioritize collections of higher historical value or with high demand for access.

Declassification review processes are built and operated to accept no risk in reviewer decision-making—a much more conservative process than is prescribed by the current Executive Order. There remains an institutional culture where reviewers routinely exempt information from declassification without actually considering whether harm will occur if it were released. This practice of managing the declassification system to zero risk wastes valuable resources and extends secrecy without justification.

There are significant policy benefits from declassification that can aid national security decisions and diplomacy. Declassification is a valuable information sharing tool, particularly when information holders must partner with stakeholders outside the intelligence and defense communities. Information may be the newest and most important policy tool of the modern era, with declassification during operations offering a strategic advantage. Public release not only makes policymakers accountable for their decisions and actions; it also affords agencies the opportunity to correct misinformation in the public domain and bolster their position in current debates. Nonetheless, declassification review is perceived by agencies as an historical exercise with very limited relevance to today's national security mission, making declassification a significantly under-resourced and under-appreciated function.

Declassification performs a service crucial to democratic society, informing citizens and promoting responsible dialogue between the public and Government. As dramatic changes take place in the information landscape, so the public's expectations are changing as well. The public, now fluent in digital technology and communication, is accustomed to timely information and expects improved access to Government information. The denial or loss of access to historically valuable records is a real concern. National security and democratic values are not separate and cannot be treated as conflicting. The new realities of the digital age require agencies modernize their declassification practices to meet the needs of all information users.

"The opportunity to change the classification system comes at an important point in our history. In this post Cold War period, we can move away from a strategy that has been characterized as something close to total risk avoidance and develop instead an approach more clearly based on risk management."

Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994, Joint Security Commission

RECOMMENDATIONS *for* TRANSFORMING DECLASSIFICATION

[RECOMMENDATION 7]: *The classification status of Formerly Restricted Data (FRD) information should be re-examined. A process should be implemented for the systematic declassification review of historical FRD information.* As designated by the Department of Energy under provisions of the Atomic Energy Act, FRD information is classified information that has been removed from the Restricted Data category after the Departments of Energy and Defense jointly determine that it relates primarily to the military utilization of atomic weapons and can be adequately safeguarded in a manner *similar* to national security information.[27] FRD information primarily concerns the military utilization of nuclear weapons, including storage locations and stockpile information. Restricted Data (RD) information is defined by the Atomic Energy Act as information concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; and the use of special nuclear material to *generate* electricity.[28] FRD information, along with RD information, is automatically excluded from declassification review under the current Executive Order.[29]

Historical FRD information, created from the end of World War II through the end of the Cold War, is often obsolete and no longer has any military or operational value. Because FRD information is the joint equity of the Department of Energy and the Department of Defense, attempts at review of this information are complex.[30] There are also high costs associated with having competing classification systems controlling access to obsolete information regarding deployment of nuclear weapons, generating confusion when users from the agencies are asked to interpret two sets of policies, guidance and procedures.

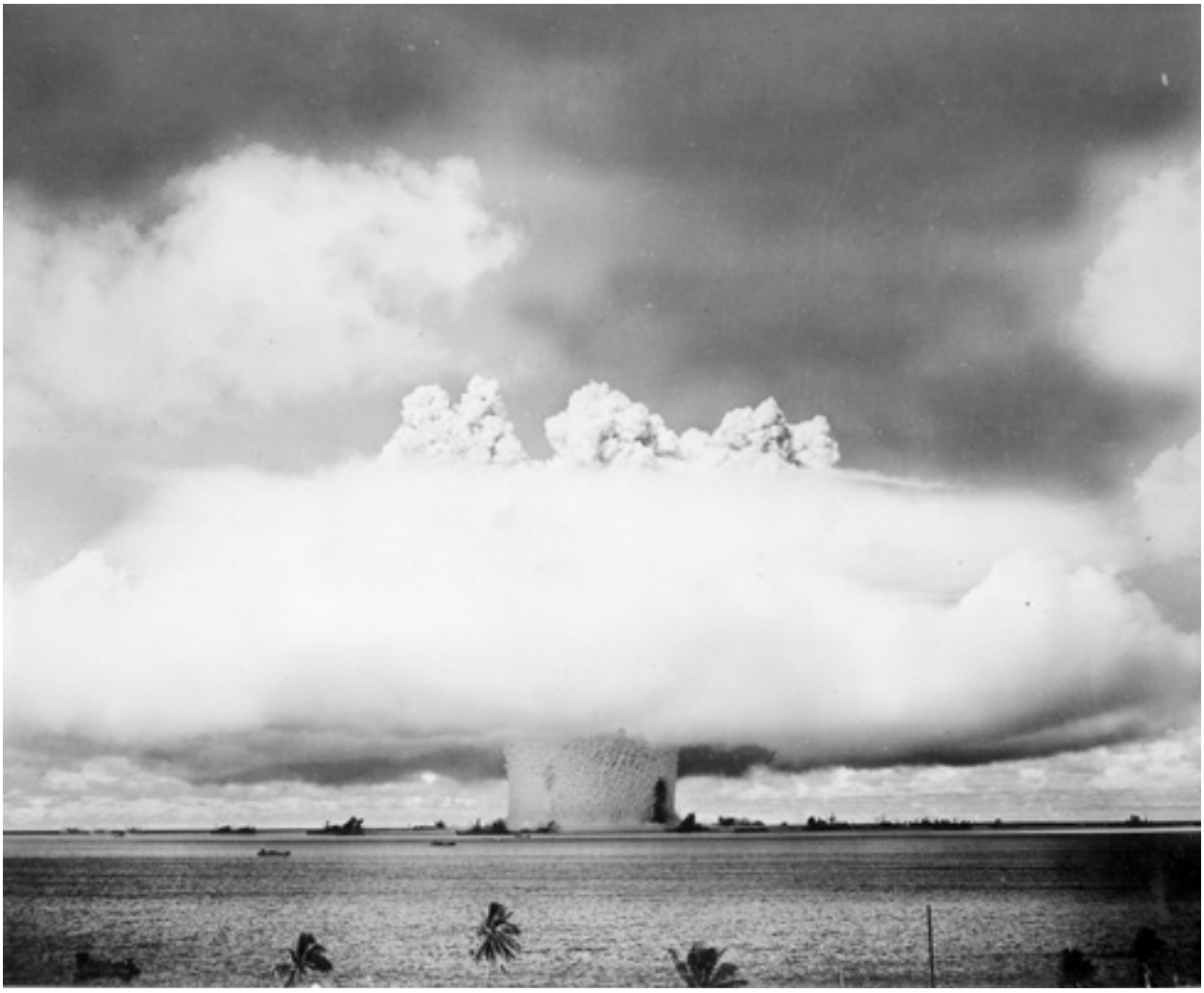
This type of information is of high interest to historians studying the Cold War, including US nuclear policy. Yet, Government regulations require that it be afforded special safeguarding and protection. At present, existing processes have had little effect in declassifying historical nuclear policy information. Requests for this information from classified files are routinely denied. The public does not understand this arcane policy, especially when so much historical nuclear policy information is in the public domain.

DURING THE CUBAN MISSILE CRISIS OF OCTOBER 1962, THE UNITED STATES

confronted the Soviet Union over the deployment of Soviet nuclear weapons in Cuba. On October 14, 1962, a U.S. Air Force U-2 photoreconnaissance plane photographed Soviet missile launch facilities under construction in Cuba. The launchers were designed for medium- and intermediate-range ballistic nuclear missiles capable of reaching most of the continental United States.

The ensuing crisis is widely considered to be the most dangerous episode of the Cold War, coming closest to an actual nuclear conflict. The U.S. demanded removal of the launchers and imposed a naval blockade of Cuba. The Soviet Union balked at U.S. demands, and President John F. Kennedy and his administration expected military action. Secret negotiations ended the crisis. The Soviet Union agreed to remove missiles from Cuba, and the United States agreed to give up unneeded missile sites in other countries.

The Cuban Missile Crisis is a critical event in Cold War history, yet key information about the negotiations and settlement fifty years ago have not been declassified due to restrictions on access to FRD information. Although inaccessible and still officially classified, much of this information is available from sources outside of the U.S. Government – a factor that contributes to public cynicism about classification.

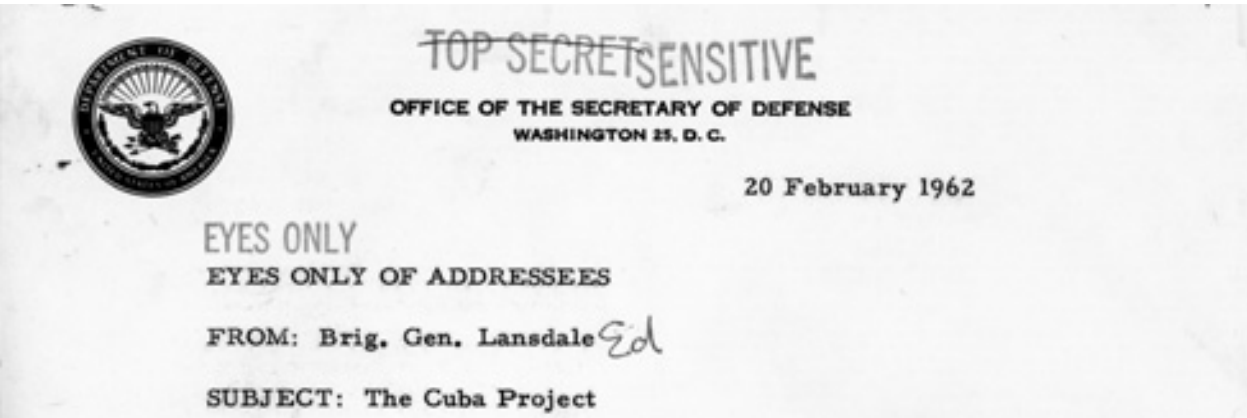


Given these complexities, the Departments of Energy and Defense should consider appropriate conversion of historical FRD information to classified national security information or to RD information.[31] FRD records converted to classified national security information would be subject to the requirements of Executive Order 13526, including the provisions for declassification. Agencies would have the authority to declassify or exempt this information from declassification, based on content. In addition to reconsidering the declassification of historical FRD information, larger reforms in the declassification strategy across government are needed, including an acknowledgement from agencies that changes to legislation may be necessary to streamline policy and practice to aid all users.

[RECOMMENDATION 8]: *The President should bolster the authority and capacity of the National Declassification Center with specific measures to advance a government-wide declassification strategy.*

[8A], *Executive Order 13526 should be amended to eliminate the additional three years now permitted for review of multiple agency equities in all archival records (including those stored outside the NDC).*[32] Eliminating the additional time for multiple-agency declassification review will compel agencies to integrate and change their declassification processes. It will facilitate and improve public access to important historical records. Since the current backlog of 400 million pages must be reviewed for declassification by the end of 2013, implementing this change should be an imperative.

[8B], *The requirement of agencies to share declassification guidance with other classifying agencies and the NDC should be strengthened. Retention of agency declassification*



~~TOP SECRET~~SENSITIVE

OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON 25, D. C.

20 February 1962

EYES ONLY

EYES ONLY OF ADDRESSEES

FROM: Brig. Gen. Lansdale Ed

SUBJECT: The Cuba Project

authority should be contingent upon sharing agency guidance. Sharing guidance enables better identification of classified information created by other agencies and results in more accurate referrals. Agencies that do not share declassification guidance should waive their right to review their information equities found in archival records containing multiple agency equities. Some agencies currently adhere to the requirement to share guidance and these agencies should be recognized and serve as models of "best practice" for inter-agency declassification cooperation.[33]

Enhancing the requirement to share guidance with other classifying agencies and eliminating the additional three years now permitted for reviewing referred records should reduce unnecessary referrals and allow more information that is no longer sensitive to be declassified. The referral system functions under the basic tenet that reviewers from all agencies have the knowledge and expertise to recognize information equities of other agencies. The ability to question agency counterparts is an important tool to assist reviewers in identifying equities, particularly for staff at the NDC where reviewers from multiple agencies are co-located. This organizational strategy will facilitate more accurate declassification reviews and limit referrals to those only absolutely necessary. Training programs should address greater inter-agency coordination across declassification programs.[34] Declassification guidance must also be kept current. Agencies should take advantage of technology to ensure guidance is accurate, reflects current mission needs, and is readily available to sister agencies.

[8C], *The President should direct Agencies to consult the NDC before prioritizing their records for declassification and transfer to the National Archives.* Prioritization plans should align with records schedules jointly created by agencies and the National Archives that direct the transfer of legal and physical custody of those records to the National Archives.

The age of the records, their historical significance, their public interest and their likelihood of declassification, should influence how and when the records are reviewed and transferred to the National Archives.[35] Once the records are transferred to the National Archives, the NDC should coordinate review of additional access provisions and restrictions and complete archival processing. Like declassification decisions, access provisions and restrictions on transferred records should be assessed with an appropriate level of risk tolerance. This would streamline one component of archival processing that currently delays the release of records to the public. The NDC should facilitate a dialogue with historians to assist agencies, policymakers, records officers, archivists, and declassification reviewers in setting priorities to improve public access to historical records.

[8D], *The Interagency National Declassification Center Advisory Panel (NAP) should have representation from the public, including representation from the Government Openness advocacy community.* Since its inception, the NDC has actively engaged the public and solicited comments in determining processing priorities and planning for future work. Additional public representation will improve transparency of NDC actions, provide important new perspectives to Government members and allow for greater public confidence. Currently, the NDC Director receives policy advice and guidance from the

inter-agency NDC Advisory Panel. The NDC Director also receives advice from an inter-agency Program Management Team (PMT) that assists the NDC in evaluating new business processes used to review records for declassification. The Board recommends these advisory groups be expanded to include public members with the knowledge and expertise to represent non-governmental interests, to help design processes to review large volumes of electronic records, to aid in re-engineering of procedures across agencies and to validate the work of the NDC to external stakeholders.

[8E], *An inter-agency effort to develop new declassification review processes should be coordinated by the NDC and be based on a risk management approach.* New processes are needed to enable agency reviewers to focus their reviews on the most sensitive records series and to cope with large volumes of digital records.[36] A risk management approach to declassification carries clear implications for classification policy and procedures and should help drive a coherent approach to risk tolerance in each part of the security classification system. Such a risk management model should also recognize that not all classified information carries the same risks or requires the same protection, and thus different levels of declassification rigor would be appropriate. It should direct limited resources to focus on reviewing information of historical significance, but which is still likely to be highly sensitive and damaging to the national security if released without careful review. External factors, such as changing world circumstances and policy determinations, should also be weighed when considering declassification review procedures for certain records series. Managing risk in the declassification process depends largely on having available for reviewers current and detailed guidance, examples of (and stated rationales for) previous declassification decisions and subject matter experts who can aid declassifiers in reviewing technical or highly specialized and sensitive information. Adopting new policies to manage risk appropriately will allow a greater volume of records to be reviewed for public access, conserve limited resources, facilitate cultural changes needed for acceptance by the declassification experts and ensure agency resources are focused on their most sensitive information.

[RECOMMENDATION 9]: *Historically significant records should be identified and set aside as early as possible after their creation to ensure their preservation, long-term access and availability to agency policymakers and historians. Each agency should have an in-house history staff to assist agency records officers and declassifiers in the prioritization of records.* Through the use of existing technologies, including data tagging, historically significant records should be prepositioned for review and timely public release. Selection of these records should reflect a reasoned judgment as to what information will be of the most interest to the public or future policymakers. Expedited access to these historical records will aid policymakers in retrieving the documentary records of past policy decisions, lending context to contemporary decision-making while cataloging valuable information for future analysis and public release. Such material not only informs public discussion of historical decisions and policies, but is also intrinsically important in documenting the Government's national security history. For these reasons, it is most desirable to bring this information into the public domain as early as possible. Agencies should understand that, if information of this level of historical significance must remain classified for some period of time, at least some of it should be analyzed, studied, and prepositioned by historians at the classified level until

FOR EXAMPLE, THERE ARE RECORDS SERIES THAT ARE RETAINED IN RECORDS *storage facilities by agencies for fifty years, while they are reviewed for declassification at twenty-five years in anticipation of the automatic declassification deadline requirements of E.O. 13526. Because these reviewed records are not yet transferred to the National Archives, they remain inaccessible and undiscoverable to the public. Some of these records series are of high researcher interest, and synchronizing their transfer schedules and declassification review would result in improved public access.*

such time as it qualifies for full declassification. Some agencies currently support an in-house history staff and should be recognized as models of "best practice" for fledgling history programs in other agencies.

[RECOMMENDATION 10]: *Agencies should improve records management overall by supporting and advancing the government-wide information management practices found in the President's Memorandum on Managing Government Records and its Directive.*[37] The President's Memorandum on Managing Government Records and its Directive recognize that effective records management practices are essential to enable access to valuable Government information and that the release of historically significant records must be a first priority under new cross-agency records management policy. The ability of agencies to transfer archival records to the National Archives for public release depends to a great degree on how efficiently agencies manage and organize their records in the first place.[38]

Implementing an effective risk management procedure that utilizes page-by-page, line-by-line reviews only when warranted depends on having confidence that the records officers have produced an accurate description of the content found in agency folders, files, boxes, and cabinets. The records management process is vital to an agency's ability to review its records of permanent value and facilitate timely release using an appropriate risk management strategy. Legislation and statutory guidelines addressing records management policies should be modernized to reflect the evolving definition of what constitutes a federal record and what portion of those federal records are permanently valuable records.[39] As agencies continue to use information technology systems to store their information and defining and identifying permanently valuable records in these systems becomes more complex, improvements in records management practices are imperative.

[RECOMMENDATION 11]: *The organization and integration of agency declassification programs must be improved across Government.* The Board recommends that declassification programs be aligned around "centers" that bring declassification reviewers and agency historians together more closely and earlier to undertake a range of case studies, outreach, and production of interdisciplinary and cross-departmental storytelling.[40] Better organization should result in improved historical understanding. Agencies should link their historians with their policymakers, classifiers, declassification reviewers, and records officers to promote the identification of permanently valuable information. As a result, outside public and private interests should ideally become more knowledgeable about the inner workings of Government agencies.

[RECOMMENDATION 12]: *Agencies should be encouraged to prepare case studies and national security histories, in classified and unclassified versions.* These studies may aid policymakers and current mission activity through a "lessons learned" perspective, while simultaneously informing the historical record of agency policies and practices. Classified histories should be reviewed for declassification at specified intervals to promote the earliest release to the public consistent with national security interests.

[RECOMMENDATION 13]: *A series of pilot projects should be used to evaluate proposals for enhancing capabilities at the NDC, streamlining the declassification system and improving access to historically significant records, including historical nuclear information*. These projects should be used to test the practicability and wisdom of the Board's recommendations and garner best practices for future implementation. In addition to the resources allocated to the NDC, these pilots should be conducted within agencies' declassification programs, employing the full range of resources available while sharing results and findings across all agencies, and with the public. The projects should concentrate on potential benefits from the enhanced use of technology, outlined in the following section.

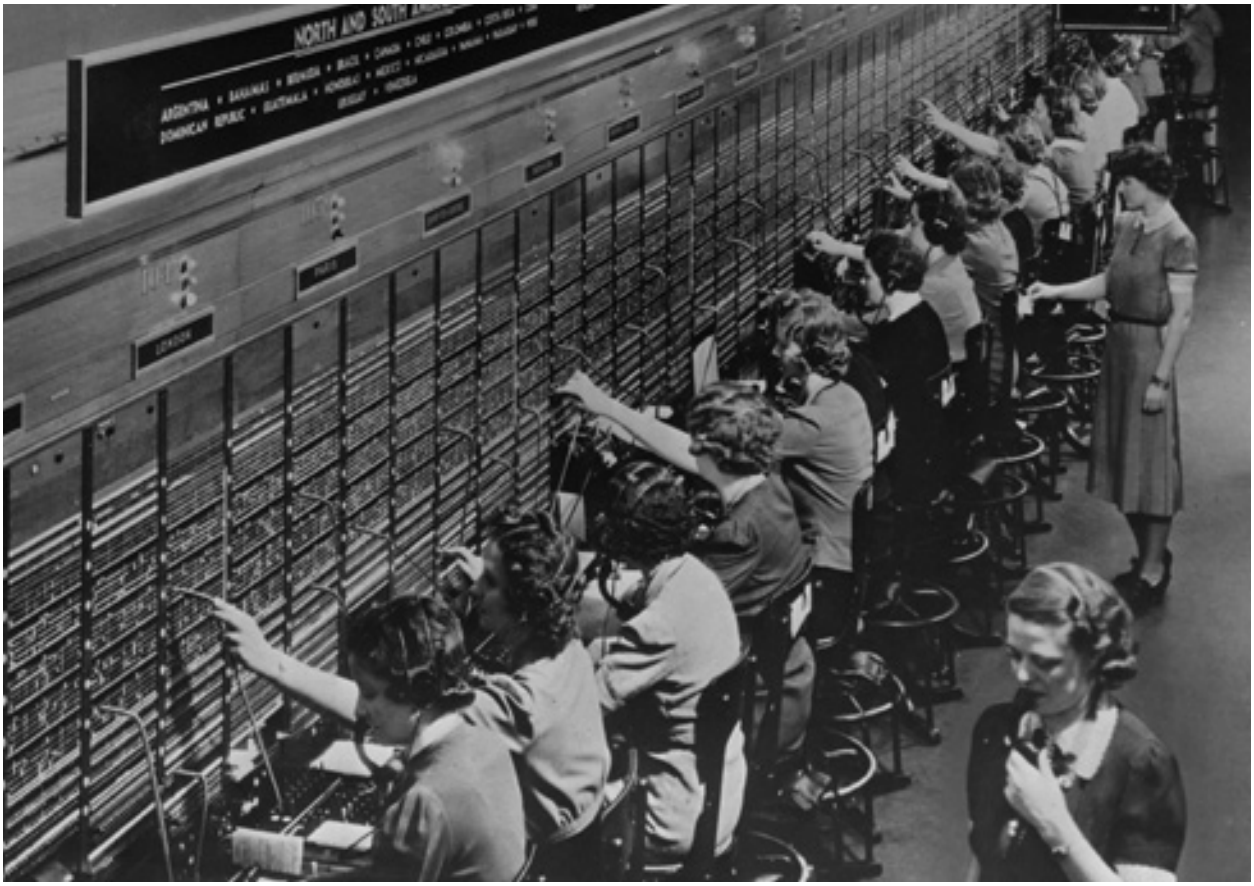
USING TECHNOLOGY *to* AID CLASSIFICATION *and* DECLASSIFICATION

The digital age has revolutionized the way information is created, stored, transmitted, and accessed. Processes for classification, declassification, and records management have not kept pace. Defining a record based on informational, evidentiary, intrinsic, and historical value is much more complicated in the digital environment, often creating all-or-nothing retention practices at agencies because of outdated guidance that does not address the complexities of streaming data creation, platform generation, or the other complexities of the emerging "Big Data" era.[41] Management and preservation of electronic records are of serious concern to agencies, as are the overwhelming volume of records awaiting review and the complexity of record formats. These factors all conspire to make the costs of manual declassification review prohibitive.

In the digital age, the approach to managing historical records requires much foresight. The many complexities of information creation and dissemination may mean we have to redefine permanently valuable records, in order that agencies have the guidance needed to identify and preserve historically significant information buried in a mass of digital information. The Government is only now entering the digital records era in their declassification processes, and the nature and character of contemporary information technology and communications offer both challenges and promise.

The search for technological solutions to classification and declassification problems must be driven by a larger vision that brings together all the component processes in the security classification system. Solutions will have to emerge from collaboration among technologists, archivists and records officers, human factors experts, historians, and national security departments and their classifiers and declassification reviewers. Reforms need to accommodate the requirement for continued improvement in government efficiencies, driven by what will likely be a resource-constrained future, but one where modern technology is essential to declassification and data discovery processes of all types.

Agencies face the rapid obsolescence of formats as paper records transition to digital media. Methods of preservation and access to old records will necessarily have to yield to innovative and sometimes costly strategies to make the transition. This extends beyond just email and current textual media, to the expanding world of audio, video, imagery, graphics, and video/audio-teleconferencing where many decisions of historical significance are made and little is now preserved for future access.



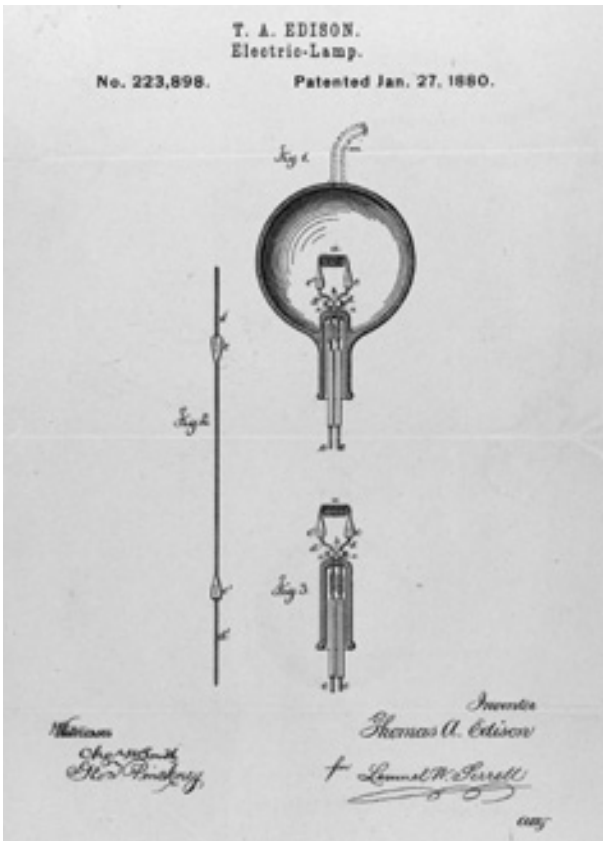
Technological innovation is simply a matter of necessity in order to achieve transformation in classification and declassification. Existing technologies, such as predictive analytics, automated metadata creation, content clustering, and context accumulation, may enhance consistency in classification and declassification, facilitate rapid information retrieval, improve information security, and hasten declassification in the electronic environment.[42]

Metadata are especially critical to future high-speed data manipulation. Users must understand how metadata are generated and used in a system, and be able to distinguish the varying levels of classification found in metadata tags. Highly classified metadata should be studied to determine their usefulness in understanding the information they describe and in their ability to aid access to that information. Because the sensitivity of highly classified metadata is likely to outlive the sensitivity of the information they describe, such metadata may need to be segregated from unclassified metadata in order to facilitate information sharing and declassification. Great promise comes with the digital era for data and metadata tagging, indexing and cross-indexing, searching, mass storage, inference, and other rules-based applications to assist declassification, access, convergence, and aggregation of media, and access by historians and public interest activities. Progress will require agencies to collaborate on policy, to share technologies, to promote best practices, and to develop common standards.

[RECOMMENDATION 14]: *The President should direct the Security Classification Reform Steering Committee to encourage collaboration and to determine how to employ existing technologies, and to develop and pilot new methods to modernize classification and declassification.* Pilot projects that test new technological solutions should inform a government-wide technology strategy for classification and declassification that will thoroughly streamline information management and access for all system users and, after declassification, for the public. Beginning at the NDC, these projects should be designed to advance the objectives of a transformed classification system. The projects should move forward as quickly as possible and, based on results, be expanded and deployed

at several agencies. The ultimate goal of the pilot projects is to discover, develop, and deploy technology that will:

- Automate and streamline declassification and classification processes, and ensure integration with electronic records management systems.
- Provide tools for preservation, search, storage, scalability, review for access, and security application.
- Address cyber security concerns, especially when integrating open source information into classified systems.
- Standardize metadata generation and tagging, creating a government-wide metadata registry, drawing on lessons learned from the intelligence community.
- Accommodate complex volumes of data (e.g. email, non-structured data, and video teleconferencing information).
- Advance government-wide information management practices by supporting the President's Memorandum on Managing Government Records.[43]



CONCLUSION

Policymakers have the opportunity to transform the classification and declassification system. Their actions will improve security, increase democratic discourse, and conserve valuable resources. The recommendations in this report require leadership, a detailed implementation strategy and vigorous oversight to ensure success. Transformation of the security classification system will take time and resources and a commitment to shift the culture from primarily risk aversion to risk management and information sharing. This will entail fundamental changes across all agencies in how information is viewed and valued, how it is accessed and preserved, and how it is managed and safeguarded. A balanced security classification system will maintain the secrecy necessary to protect national security and at the same time assure the transparency and openness required in and for a democratic society.

To make classification and declassification functional for the future, respected by users, and trusted by the public, longstanding policy and practice must change. Staying the present course will prove exceedingly difficult, costly, and even damaging to national security. Technology and the rapid growth of digital information, in particular, places extraordinary stresses on the current classification system beyond anything that could have been anticipated when the system was created. Paper-based protocols developed seventy years ago no longer suffice.

To meet contemporary challenges, the Government needs a fresh approach. Abandoning outdated attitudes and embracing a new vision will transform the Government's ability to manage secrecy, accomplish the national security mission, and appropriately inform the public. Transforming the classification system will not happen overnight. It will take time, resources, and commitment. The way forward will require a fundamental change in how American society and its Government understand, manage, safeguard, and preserve Government information.


IN CONGRESS, JULY 4, 1776.

A DECLARATION

BY THE REPRESENTATIVES OF THE

UNITED STATES OF AMERICA,

IN GENERAL CONGRESS ASSEMBLED.

WHEN in the Course of human Events, it becomes necessary for one People to dissolve the Political Bands which have connected them with another, and to assume among the Powers of the Earth, the separate and equal Station to which the Laws of Nature and of Nature's God entitle them, a decent Respect to the Opinions of Mankind requires that they should declare the causes which impel them to the Separation.

We hold these Truths to be self-evident, that all Men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the Pursuit of Happiness.—That to secure these Rights, Governments are instituted among Men, deriving their just Powers from the Consent of the Governed, that whenever any Form of Government becomes destructive of these Ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its Foundation on such Principles, and organizing its Powers in such Form, as to them shall seem most likely to effect their Safety and Happiness. Prudence, indeed, will dictate that Governments long established should not be changed for light and transient Causes; and accordingly all Experience hath shewn, that Mankind are more disposed to suffer, while Evils are sufferable, than to right themselves by abolishing the Forms to which they are accustomed. But when a long Train of Abuses and Usurpations, pursuing invariably the same Object, evinces a Design to reduce them under absolute Despotism, it is their Right, it is their Duty, to throw off such Government, and to provide new Guards for their future Security. Such has been the patient Sufferance of these Colonies; and such is now the Necessity which constrains them to alter their former Systems of Government. The History of the present King of Great-Britain is a History of repeated Injuries and Usurpations, all having in direct Object the Establishment of an absolute Tyranny over these States. To prove this, let Facts be submitted to a candid World.

He has refused his Assent to Laws, the most wholesome and necessary for the public Good.

He has forbidden his Governors to pass Laws of immediate and pressing Importance, unless suspended in their Operation till his Assent should be obtained; and when so suspended, he has utterly neglected to attend to them.

He has refused to pass other Laws for the Accommodation of large Districts of People, unless those People would relinquish the Right of Representation in

A Vision for a Classification and Declassification System of the Future:

ONE EXAMPLE *of a* FUNCTIONING SECURITY CLASSIFICATION SYSTEM

As an agency official creates an electronic record, an automated tool assists the official by reviewing the record's content, comparing it to previously unclassified, classified, and declassified records, and suggests an appropriate classification level, if any, and corresponding markings. When the official disagrees with the system's prompt, the record is referred to information security personnel and original classification authorities for deliberation. The results of this classification review are ingested into the system, which immediately identifies all existing and future appearances of comparable information and marks it accordingly.

The system imprints all records with standardized metadata, which chronicle the record's authorship, sources, and access controls, as well as its reasons for classification and its declassification instructions. The digital signatures of credentialed personnel who access the record are captured in its transaction history. Security managers audit record access histories to protect against insider threats and ensure appropriate access. Agency records officers and historians identify and digitally annotate historically significant file series, which are used to compose classified and unclassified agency histories.

Metadata facilitate the rapid retrieval of information to fulfill mission requirements, assist in preemptive disclosures, and honor public requests. If a record is not already declassified after discretionary review, its access restrictions and classification automatically self-extinguish as it reaches its declassification date. Records deemed historically valuable but exempt from automatic declassification are prioritized in eventual systematic declassification reviews.

To prevent referral backlogs and encourage a historical perspective, all exempted records are reviewed for declassification at the National Declassification Center (NDC). Agency reviewers at the NDC conduct systematic and mandatory declassification reviews and input the results to expand the system's contextual knowledge. Pass-fail reviews of classified records are a thing of the past; the sophistication and automation of the system allows all declassification reviews to be conducted at the redaction level. Records containing Formerly Restricted Data information are eligible for declassification review at the NDC after 25 years. At the request of respective Congressional committees, classified House and Senate records are also systematically processed for declassification at the NDC.

Information flows readily and effectively between policymakers, users, records managers, and historians and, through efficient and accurate declassification, to the public. Technology and procedural reforms make classification consistent and declassification timely. Advanced information retrieval and analysis tools are used to address over-classification in a comprehensive, real-time manner, and changes in classification precedent are immediately and comprehensively implemented. The centralization of government work processes and the renewed emphasis on openness increase the public's confidence in the security classification system and reinforce the fact that national security information belongs to the American people.

ENDNOTES *for* RECOMMENDATIONS

Endnotes i-x for Executive Summary on page 5.

[1] See Endnote x.

[2] *Improving Declassification, A Report to the President from the Public Interest Declassification Board*, (*http://www.archives.gov/declassification/pidb/improving-declassification.pdf*), January 2008.

[3] See Endnote iii: section 3.7.

[4] See Endnote i.

[5] *Transforming Classification*, (*http://blogs.archives.gov/transformingclassification/*), March 2011.

[6] See Endnote iii: sections 1.1 and 1.2.

[7] When he signed Executive Order 13526, the President mandated agencies to undertake a Fundamental Classification Guidance Review to review the accuracy of their current classification guides. He required agencies to complete their reviews by June 27, 2012 and submit their final reports to the Information Security Oversight Office (ISOO). See Endnote iii: section 1.9.

[8] See Endnote ii.

[9] The Information Security Oversight Office (ISOO) is engaged in dialogue with United Kingdom counterparts on the topic of simplifying and rationalizing information security policy in our respective governments. United Kingdom experience has shown that the proliferation of levels of classification and methods of restriction require redress to reduce costs and improve information sharing access across Government. As a result, the United Kingdom is formally developing a new classification model that contemplates using only two levels of classification. In addition, United Kingdom officials have engaged other Commonwealth partners on these topics and found similar efforts to identify and adopt a streamlined classification system.

[10] As part of its study, the Board found that information classified as Confidential is created, stored, disseminated and safeguarded on Secret systems in the current classification system.

[11] See Endnote v.

[12] Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq. See also End*note iii: section 6.2 and Endnote 30.*

[13] The classified electronic network systems for the intelligence and defense communities are the Joint Worldwide Intelligence Communications System (JWICS) and the Secret Internet Protocol Router Network (SIPRNet). The unclassified electronic network system is the *Unclassified but Sensitive Internet Protocol Router Network (NIPRNET).*

[14] Agencies have established procedures under which authorized holders of information, including authorized holders outside the classifying agency, are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. Classification challenges rarely occur as reported in ISOO's Annual Report to the President. See Endnote iii: section 1.8 and Endnote v.

[15] Under the auspices of the National Declassification Center, the implementing directive of E.O. 13526 allows agencies up to three years to complete a review their information for declassification. See 32 C.F.R. Parts 2001 and 2003 Classified National Security Information; Final Rule, section 2001.34.

[16] A digital asset is digital content owned by an individual or organization. Digital assets are any digital material owned by an enterprise or individual including text, graphics, audio, video, and animations. Digital content includes individual files such as images, photos, videos, and text files, and also other digital content, such as data in a database. Today, enterprises have a huge amount of digital assets that require managing. PC Magazine, (*http://www.pcmag.com/encyclopedia_term/0,1237,t=digital+asset&i=41283,00.asp*), Copyright © 1981–2012, The Computer Language Company, Inc.

[17] One intelligence agency estimates that one terabyte of data is equivalent to approximately 112 million pages of information.

[18] "How Large is a Petabyte?" GIZMODO Storage. (*http://gizmodo.com/5309889/how-large-is-a-petabyte*), July 2012.

[19] Digital Preservation Management Workshop, Cornell University Library. Digital Preservation Management: Implementing Short-Term Strategies for Long-Term Solutions, online tutorial developed for the Digital Preservation Management workshop, developed and maintained by Cornell University Library, 2003-2006; extended and maintained by ICPSR, 2007-on. (*http://www.dpworkshop.org/index.html*), 2012.

[20] See Endnote iii. Predecessor orders to E.O. 13526 include Executive Order 12958 of April 17, 1995, and its amendment, Executive Order 13292 of March 25, 2003.

[21] Public Interest Declassification Board's Letter to the President, March 6, 2009. (*http://www.archives.gov/declassification/pidb/letter03-06-09.pdf*) 2012.

[22] See Endnote iii: section 3.7.

[23] The Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a, as amended.

[24] The President gave the NDC a December 31, 2013 deadline to review for declassification and process for release the 400 million page backlog of archival records. See Endnote i: section 2.

[25] The NDC streamlined its declassification review process by using the Six Sigma business philosophy to focus on meeting customer requirements and sustaining business products and services. The Six Sigma business management strategy seeks to improve the quality of process outputs by identifying and removing the causes of defects (errors) and minimizing variability in manufacturing and business processes. It uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Black Belts", "Green Belts", etc.) who are experts in these methods. Antony, Jiju. "Pros

and cons of Six Sigma: an academic perspective". Archived from the original on July 23, 2008. Retrieved August 5, 2010.

[26] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*. New York: W.W. Norton & Company, 2004.

[27] Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq.: section 142 and 10 C.F.R. PART 1045 Nuclear Classification and Declassification; Final Rule, section 1045.3.

[28] Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq.: section 11 10 C.F.R. PART 1045 Nuclear Classification and Declassification; Final Rule, section 1045.3.

[29] See Endnote iii: section 6.2.

[30] The Atomic Energy Act of 1954 gives equity to the Department of Energy over all atomic energy and nuclear information, and stipulates that this information is automatically classified in a separate system. The two classification categories—RD and FRD—were created pursuant to the Atomic Energy Act and its implementing regulation 10 C.F.R. 1045, Nuclear Classification and Declassification. There was recognition that it was imperative to closely safeguard and protect information on the design of nuclear weapons. There was also recognition that, while the military did not need to know how to design and build a weapon, it had the responsibility to safeguard, maintain, and plan for use of the actual weapons. Thus, the implementing regulations to this act specify that FRD information is to be administered jointly by the Department of Energy and the Department of Defense.

[31] See Endnote vi.

[32] See Endnote 15.

[33] See Endnote iii: section 3.7 (b) (3).

[34] See Endnote iii: section 3.7 (b) (4).

[35] Although the President's Memorandum on Managing Government Records and its Directive requires senior agency officials to identify records for eventual transfer to the National Archives, the agencies should also be required to collaborate with records officers from National Archives and the NDC to develop prioritization plans that ensure timely transfer of records for improved access to historically significant records. See Endnote x, section 2.

[36] See Endnote 16, "A Snapshot of the Looming Digital Challenge."

[37] See Endnote x.

[38] The Board learned there are cases when information is so tightly controlled that agency records officers are prohibited clearance or access, and consequently are unable to evaluate the records.

[39] Contemplation of recommendations regarding records management practices should include determination if legislative changes are needed, specifically regarding the Federal Records Act of 1950, as amended, and the Presidential Records Act. The Federal Records Act of 1950, as amended, codified at 44 U.S.C. Chapters 29, 31 and 33, *establishes the framework for records management programs in Federal Agencies. It was last amended on* October 21, 1976. The Presidential Records Act of 1978, codified at 44 U.S.C. Chapter 22, governs the official records of Presidents and Vice Presidents created or received after January 20, 1981. It mandates the preservation of all presidential records, changing the legal ownership of the official records of the President from private to public, and implements a new statutory structure under which all presidential records must be managed. It has not been amended.

[40] "Center concepts" in this context refers to the declassification programming and prioritization plans associated with historical centers that operate across Government. This alignment will ensure interagency and across-agency collaboration. Some examples include the National Declassification Center and the Center for the Study of Intelligence.

[41] See Endnote 39.

[42] Context accumulation is the incremental process of relating new data to previous data and remembering these relationships, for improved data accuracy. It is an advanced computing process related to entity analytics in which a system is able to predict relevance and importance dynamically, based on the accumulation and persistence of context produced by ingested data. Algorithms are generated using this contextual data and then employed to determine whether newly introduced data have a place or relationship with historical data. Once this determination is made, the system then saves and uses this new observation when evaluating other introduced data. Source: *Using Entity Analytics to Greatly Increase the Accuracy of Your Models Quickly and Easily,* 2012, IBM®, Redbooks®, (*http://www.redbooks.ibm.com/redpapers/pdfs/redp4913.pdf*).

[43] See Endnote x.

APPENDIX A

PUBLIC INTEREST DECLASSIFICATION BOARD MEMBER BIOGRAPHIES

Presidential Appointees

NANCY E. SODERBERG (CHAIR) was reappointed by the President as Chair on November 16, 2012. She is a national security expert with experience at the White House, United Nations, and Congress. While at the National Security Council, she worked extensively on declassification issues. She is currently the President of the Connect U.S. Fund, a non-profit organization that focuses on promoting U.S. global engagement. In addition, she is a Distinguished Visiting Scholar at the University of North Florida and the President and CEO of Soderberg Global Solutions. Ambassador Soderberg served as Vice President of the International Crisis Group from 2001 until 2005. She was the U.S. Representative for Special Political Affairs at the United Nations from 1997 to 2001, and Staff Director of the National Security Council and Deputy Assistant to the President from 1993 until 1997. From 1985 to 1992, she served as a Foreign Policy Advisor to Senator Edward M. Kennedy. Ambassador Soderberg has written *The Superpower Myth: The Use and Misuse of American Might* and co-authored, with Brian Katulis, *The Prosperity Agenda: What the World Wants from America —and What We Need in Return*. She is a member of the Council on Foreign Relations. She earned a B.A. from Vanderbilt University and an M.S. from Georgetown University's School of Foreign Service. Ambassador Soderberg is serving her second term on the Board.

MARTIN C. FAGA was reappointed by the President on February 10, 2012. He was the President and Chief Executive Officer of The MITRE Corporation for six years, retiring in 2006. Before joining MITRE, Mr. Faga served as Assistant Secretary of the Air Force for Space from 1989 until 1993. At the same time, he served as Director of the National Reconnaissance Office, responsible to the Secretary of Defense and the Director of Central Intelligence for the development, acquisition, and operation of all U.S. satellite reconnaissance programs. Mr. Faga has been awarded the National Intelligence Distinguished Service Medal, the Department of Defense Distinguished Public Service Medal, the Air Force Exceptional Civilian Service Medal, and the NASA Distinguished Service Medal. In 2004, he was awarded the Intelligence Community Seal Medallion. He was first appointed to the Board in October 2004, and again in January 2009. He has also served on the President's Intelligence Advisory Board. Mr. Faga graduated from Lehigh University with a B.S. and an M.S. in electrical engineering. He is serving his third term on the Board.

WILLIAM H. LEARY was appointed by the President on February 10, 2012. He was the Special Adviser to the National Security Advisor and Senior Director for Records and Access Management on the National Security Staff until his retirement in 2011. In that capacity, he served as Chair of the Interagency Security Classification Appeals Panel and Chair of the Records Access and Information Security Interagency Policy Committee. A strong proponent of governmental transparency, Mr. Leary was one of the primary executive branch officials behind the creation of the Board in 2000 and the development of President Obama's Executive Order 13526 on Classified National Security Information. Prior to joining the National Security Council staff, he served as the Deputy Director of the Agency Services Division at the National Archives and Records Administration for five years. From 1968 until 1973, Mr. Leary taught American history at the University of Virginia, the College of William and Mary, and the University of South Alabama. He received his B.A. in foreign affairs and M.A. and A.B.D. in history, all from the University of Virginia. He is serving his first term on the Board.

ELIZABETH RINDSKOPF PARKER was reappointed by the President on January 10, 2012. She is currently a professor of law at the University of the Pacific, McGeorge School of Law where she earlier served as dean from 2002-2012. Previously, she served as general counsel for the University of Wisconsin System (1999 to 2002); general

counsel to the Central Intelligence Agency (1990 to 1995); Principal Deputy Legal Adviser, U.S. Department of State (1989-1990); general counsel, National Security Agency (1984-1989) and as Acting Assistant Director (Mergers and Acquisitions) at the Federal Trade Commission. In addition to her experience managing government legal offices, Ms. Parker also served as the director of the New Haven Legal Assistance Association, Inc. (1973-1976) after handling civil rights and civil liberties litigation as a co-operating attorney with the NAACP Legal Defense and Education Fund, Inc. She has been a member of the Special Advisory Group to the Director of National Intelligence since 2009 and is a member of the Board of the Civilian Research Development Foundation-Global and the Council on Foreign Relations. Both her law (1968) and undergraduate (cum laude, 1964) degrees are from the University of Michigan. Ms. Parker is serving her third term on the Board.

Congressional Appointees

DAVID E. SKAGGS was appointed by Rep. Nancy Pelosi, Minority Leader of the House, on March 29, 2012. He is the Chairman of the Board of the Office of Congressional Ethics and practices law with the firm McKenna, Long, and Aldridge. He previously served as Executive Director of the Colorado Department of Higher Education from 2007 to 2009. He served 12 years in Congress from 1987 to1999 as the Representative from the 2nd Congressional District in Colorado, including 8 years on the House Appropriations Committee and 6 years on the House Permanent Select Committee on Intelligence. After leaving Congress, he served as Executive Director of the Center for Democracy and Citizenship at the Council for Excellence in Government from 1999 to 2006, and taught as an adjunct professor at the University of Colorado, where he recently resumed teaching as an adjunct professor at the University of Colorado Law School. He has a B.A. in philosophy from Wesleyan University and an LL.B from Yale Law School. Mr. Skaggs is serving his third term on the Board.

ADMIRAL WILLIAM O. STUDEMAN, USN (RET.) was appointed by Rep. John Boehner, Speaker of the House, on May 18, 2012. He recently retired from Northrop Grumman Corporation as Vice President and Deputy General Manager of Mission Systems. Admiral Studeman's flag tours included Office of the Chief of Naval Operations (OPNAV) Director of Long Range Navy Planning; Director of Naval Intelligence; Director of the National Security Agency; and Deputy Director of the Central Intelligence Agency, with two extended periods as Acting Director. He served as a member of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction and is currently serving on both the National Advisory Board on Bio-Security and the Defense Science Board. He holds a B.A. in history from the University of the South in Sewanee, TN, and an M.A. in public and international affairs from George Washington University. Admiral Studeman is serving his third term on the Board.

SANFORD J. UNGAR was reappointed to the Board by Sen. Harry Reid as Majority Leader of the Senate on March 7, 2011. He currently serves as the tenth President of Goucher College in Baltimore, Maryland. Prior to assuming his position at Goucher College, Mr. Ungar served as Director of the Voice of America, Dean of the School of Communication at American University in Washington, D.C., as the Washington editor of *The Atlantic,* as managing editor of Foreign Policy magazine, and as a staff writer for *The Washington Post.* He is a former host of "All Things Considered" on National Public Radio and had published six books, including *The Papers & The Papers: An Account of the Legal and Political Battle over the Pentagon Papers.* Mr. Ungar obtained his B.A. in Government from Harvard College and a Master's degree in International History from the London School of Economics and Political Science. Mr. Ungar is serving his second term on the Board.

APPENDIX B

WITNESSES APPEARING BEFORE *the* BOARD

During its study of the security classification system, the Public Interest Declassification Board met with individuals and groups from Executive branch agencies, international partners, the public interest and openness community, and the Congress. Additionally, representatives from academia, the private sector, and the media, as well as experts in the fields of technology and public policy, and individual agency classification and declassification program managers and practitioners all contributed to the Board's study.

Those individuals and groups include representatives from the following Executive branch agencies and departments:

Central Intelligence Agency
Department of Defense
- Office of the Secretary of Defense
- Joint Chiefs of Staff
- Defense Advanced Research Projects Agency
- Department of the Air Force
- Department of the Army
- Department of the Navy
- Defense Intelligence Agency
- National Security Agency
- National Geospatial-Intelligence Agency
- National Reconnaissance Office

Department of Energy
Department of Justice
- Federal Bureau of Investigation

Department of State
National Archives and Records Administration
- Office of Government Information Services

National Security Staff
Office of the Director of National Intelligence
- Intelligence Advanced Research Projects Activity

The Board also wishes to thank members of the Directorate of Security and Intelligence, Government Security Secretariat, United Kingdom, for sharing its study on the topic of transforming the UK security classification system. In particular:

- Michael Brennan, Deputy Director of the Government Security Secretariat, Cabinet Office
- Michael Shryane, Head of Policy, Government Security Secretariat, Cabinet Office

In preparing this report, the Board heard from the following individuals and groups:

- Steve Aftergood, Senior Research Analyst, Project on Government Secrecy, Federation of American Scientists
- Carol Anderson, Member, Historical Advisory Committee, Department of State
- Randy Avent, Chief Scientist, Defense Department Research and Engineering, Department of Defense (DoD)
- Jason Baron, Director of Litigation, National Archives and Records Administration (NARA) and Co-Chair of The Sedona Conference® Working Group on Electronic Document Retention and Production
- David M. Barrett, Professor, Villanova University
- John Bell, Policy Analyst, Information Security Oversight Office
- Laura A. Belmonte, Professor, Oklahoma State University and Member, State Department's Historical Advisory Committee
- Dr. Scott Bernard, Federal chief Enterprise Architect
- Tom Blanton, Executive Director, National Security Archive
- Deborah Bonanni, Chief of Staff, National Security Agency (NSA)
- Elizabeth Brooks, Associate Director for Community Integration, Policy and Records, NSA
- Edmund Brynn, The Historian (acting), Department of State
- William Burr, Senior Analyst, National Security Archive

- Neil Carmichael, Indexing and Declassification Review Director, National Declassification Center (NDC)
- William Carpenter, Lead Staff Member, Interagency Security Classification Appeals Panel
- Honorable Ashton Carter, Deputy Secretary of Defense, DoD
- Robert Chadduck, Principal Technologist for Advanced Research, NARA
- Jeff Charlston, Professor, University of Maryland University College and Former Historian, US Army Center of Military History
- Honorable James R. Clapper, Director of National Intelligence
- Nicklous Combs, Chief Technology Officer, EMC Federal; Former IT Director and Chief Information Officer of the National Media Exploitation Center, Office of the Director of National Intelligence (ODNI); and Former Deputy Chief for Enterprise IT Solutions, Defense Intelligence Agency (DIA)
- Mark Conrad, Archives Specialist, Center for Advanced Systems and Technologies (NCAST), NARA
- Harry P. Cooper, Jr. Chief of Classification Management and Collaboration Group, Central Intelligence Agency (CIA)
- Adrian Cunningham, Director, Strategic Relations and Personal Records, National Archives of Australia and Former President, Australian Society of Archivists
- A.J. Daverede, Production Division Director, NDC
- James David, Historian, National Aeronautics and Space Administration
- William Eckroade, Principal Deputy Chief for Mission Support Activities, Office of Health, Safety, and Security, Department of Energy (DOE)
- John Elliff, Former Staff Member; Church Committee, Former Staff Member, Senate Select Committee on Intelligence; and, Former Senior Executive at the Federal Bureau of Investigation (FBI)
- Brian Eshenbrenner, Director, Security and Intelligence Directorate, Defense Advanced Research Projects Agency
- Thomas A. Ferguson, Principal Deputy Under Secretary of Defense for Intelligence
- Honorable David Ferriero, Archivist of the United States, NARA
- Sharon Bradford Franklin, Senior Counsel, The Constitution Project
- Michael German, Policy Counsel on National Security, Immigration and Privacy, ACLU and Former Special Agent, FBI
- Elizabeth Goitein, Co-Director, Liberty and National Security Program, Brennan Center for Justice
- Honorable Porter Goss, Former Chair of the House Permanent Select Committee on Intelligence and Former Director of Central Intelligence
- Margaret P. Grafeld, Deputy Assistant Secretary for Global Information Services, Bureau of Administration, Department of State
- Dr. Dolly Greenwood, Director, Enterprise Engineering & ISR, MITRE
- James Hallo, Director, Corporate Security, MITRE
- Morton Halperin, Senior Advisor, Open Society Institute; Former Director of the Policy Planning Staff at the Department of State; Former Special Assistant to the President and Senior Director for Democracy, National Security Council; and Former Deputy Assistant Secretary of Defense (International Security Affairs).
- Honorable John Paul Hammerschmidt, Former Congressman and Former Member of the President's Commission on Aviation Security and Terrorism
- Honorable Kenneth B. Handelman, Principal Deputy Assistant Secretary for Global Strategic Affairs, DoD
- David Hardy, Section Chief, Record / Information Dissemination Section, FBI
- General Michael Hayden (Ret.), Former Director, NSA; Former Director, CIA; and Former Principal Deputy Director of National Intelligence, ODNI

- Steve Henry, Deputy Assistant to the Secretary of Defense for Nuclear Matters
- David Herschler, Deputy Historian, Department of State
- Douglas Hudson, Director of Special Programs, Applied Physics Laboratory, The Johns Hopkins University
- Ken Hughes, Presidential Records Program, Miller Center, University of Virginia
- Lieutenant General Patrick Hughes, (ret.) Vice President for Intelligence and Counterterrorism, L3 Communications and Former Director, DIA
- Richard H. Immerman, Professor, Temple University and Member, Department of State's Historical Advisory Committee
- Diane Janosek, Deputy Associate Director for Community Integration, Policy and Records, NSA
- Vincent Jarvie, Vice President for Corporate Security, L3 Communications
- Jeff Jonas, Chief Scientist, IBM Entity Analytics Group and IMB Distinguished Engineer, IBM
- Nate Jones, Freedom of Information Coordinator, National Security Archive
- John Judge, Founder, Committee for an Open Archives
- Fred Kaplan, Writer, Slate Magazine
- Edmund Kaufhold, Staff Member, Security Directorate, Office of the Under Secretary of Defense (Intelligence)
- Ambassador Patrick Kennedy, Under Secretary for Management, Department of State
- Jeffrey P. Kimball, Professor Emeritus, Miami University of Ohio
- Horen Kuecuekyan, Principal Software Architect, Sensis Corporation
- Vivek Kundra, Former United States Chief Information Officer, Office of Management and Budget
- Michael Kurtz, Former Acting Director, NDC
- Joseph Lambert, Director, Information Management Services, CIA
- Wayne Leathers, Defense Change Management Organization
- Tom Lee, Director of Sunlight Labs, Sunlight Foundation
- Ann Levin, Program Manager, CACI, Inc.
- Robert Litt, General Counsel, ODNI
- Brian Martin, President, History Associates
- Patrice McDermott, Executive Director, OpenTheGovernment.org
- Elizabeth A. McGrath, Deputy Chief Management Officer for the Department of Defense
- Don McIlwain, Chief, FOIA-MDR Division, NDC
- Robert McMahon, Chairman, Historical Advisory Committee, Department of State
- Carmen Medina, Former Associate Deputy Director of Intelligence, CIA
- David Mengel, Deputy Director, NDC
- Ambassador Robert Miller, Information Programs and Services, Department of State
- Nicholas Murphy, Information Programs and Services, Department of State
- Anna Nelson, Professor, American University and Former Member, John F. Kennedy Assassination Records Review Board
- Miriam Nisbet, Director, Office of Government Information Services, NARA
- R. Stan Norris, Senior Research Associate, National Defense Council
- Eric Olson, QinetiQ
- Pablo Osinaga, Co-Founder of Kormox
- Honorable Stephanie O'Sullivan, Principal Deputy Director of National Intelligence
- Trudy Huskamp Peterson, Member, Historical Advisory Committee, Department of State, Former Acting Archivist of the United States; Former Archivist, United Nations High Commissioner for Refugees; and Former Executive Director, Open Society Archives
- Honorable Daniel Poneman, Deputy Secretary of Energy, DOE
- John Prados, Senior Research Fellow, National Security Archive
- Madeline Proctor, Initial Processing and Declassification Division, NDC
- Harold Reylea, Policy Analyst, Congressional Research Service (ret.)
- Fred Riccardi, Senior Executive Director, ManTech International Corporation

- Douglas Richards, Chief, Declassification Branch, Information Management Division, Joint Staff Secretariat
- Don Richie, Senate Historian
- Alison Roach, Fried Frank Legal Fellow, The Constitution Project
- David Robarge, Chief Historian, CIA
- Mary Ronan, Director, Access Management, National Security Staff
- Lisa Rosenberg, Government Affairs Consultant, Sunlight Foundation
- Debbie Ross, DoD Information Security Policy, Office of the Under Secretary of Defense (HUMINT, Counterintelligence and Security)
- James Russell, QinetiQ
- Bob Savage, Formerly Media Preservation Unit, Stanford University Libraries and Formerly Director, Records and Institutional Research, College of Arts and Sciences, Vanderbilt University
- Daniel Schuman, Policy Counsel, Sunlight Foundation
- David Shapiro, Co-Director, Liberty and National Security Program, Brennan Center for Justice
- Michael Sheehy, Former Staff Director of the House Permanent Select Committee on Intelligence
- Sheryl Shenberger, Director, NDC
- Katherine Sibley, Member, Historical Advisory Committee, Department of State
- Nancy Smith, Director, Presidential Materials Staff, NARA
- Bob Spangler, Acting Division Director for Electronic and Special Media Records Services, NARA
- Peter Spiro, Member, Historical Advisory Committee, Department of State
- Corin Stone, Deputy Assistant Director of National Intelligence for Policy, ODNI
- Al Tarasuik, Intelligence Community Chief Information Officer
- Russell Travers, Former Deputy Director for Information Sharing and Knowledge Development at the National Counterterrorism Center
- Tom Uva, Vice President & Chief Information Officer, Sensis Corporation
- John Verdi, Senior Council and Director of Open Government Project, Electronic Privacy Information Center
- Sheryl Walter, Director of Information Programs and Services, Bureau of Administration, Department of State
- Paul Wester, Chief Records Officer, NARA
- Andrew Weston-Dawkes, Director, Office of Classification, DOE
- Lee White, Executive Director, National Coalition for History
- James Wilson-Quayle, Chief, Records, Research & Content Branch, Joint Staff Secretariat
- John Wonderlich, Policy Director, Sunlight Foundation
- Thomas Zeiler, Member, Historical Advisory Committee, Department of State
- David Zierler, Historian, Office of the Historian, Department of State

APPENDIX C

GLOSSARY

Accession: To take legal and physical custody of a group of records or other materials and to formally document their receipt. Source: *A Glossary of Archival and Records Terminology,* Copyright © 2012, Society of American Archivists, (*http://www2.archivists.org/glossary*).

Archival Processing: The arrangement, description, and housing of archival materials for storage and use by patrons. Source: *A Glossary of Archival and Records Terminology,* Copyright © 2012, Society of American Archivists, *(http://www2.archivists.org/glossary*). Archival processing Federal records at the National Archives and Records Administration also entails a review for public access. The review is necessary to remove certain information that would compromise national security, violate the privacy of a living person, or would violate a Federal statute. This Information is then indexed so researchers know what has been removed.

Automatic Declassification Review: The declassification of information based solely upon (1) the occurrence of a specific date or event as determined by the original classification authority, or (2) the expiration of a maximum time frame for duration of classification established under this order. Source: E.O. 13526, section 6.1(e).

Byte: A unit of computer information or data-storage capacity that consists of a group of eight bits and that is used especially to represent an alphanumeric character. Source: "Byte." Merriam-Webster.com. Merriam-Webster, 2011.

Classification Challenges: The challenge of classification status of information by an authorized holders of information who, in good faith, believe that its classification status is improper in accordance with agency procedures established under section 1.8 of Executive Order 13526. Source: E.O. 13526, section 1.8.

Classified national security information: Information that has been determined (pursuant to E.O. 13526, or any predecessor order) to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Source: E.O. 13526, section 6.1(i).

Content Clustering: Connecting two or more computers together in such a way that they behave like a single computer. Clustering is used for parallel processing, load balancing and fault tolerance. Clustering is a popular strategy for implementing parallel processing applications because it enables companies to leverage the investment already made in PCs and workstations. In addition, it's relatively easy to add new CPUs simply by adding a new PC to the network. Source: "Clustering." Webopedia.com. The IT Business Edge Network, 2012.

Context Accumulation: Context accumulation is the incremental process of relating new data to previous data and remembering these relationships, for improved data accuracy. It is an advanced computing process related to entity analytics in which a system is able to predict relevance and importance dynamically, based on the accumulation and persistence of context produced by ingested data. Algorithms are generated using this contextual data and then employed to determine whether newly introduced data have a place or relationship with historical data. Once this determination is made, the system then saves and uses this new observation when evaluating other introduced data. Source: *Using Entity Analytics to Greatly Increase the Accuracy of Your Models Quickly and Easily,* 2012, IBM®, Redbooks®, (*http://www.redbooks.ibm.com/redpapers/pdfs/redp4913.pdf*).

Declassification: The authorized change in the status of information from classified information to unclassified information. Source: E.O. 13526, section 6.1(m).

Derivative Classification: The incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction

of existing classified information is not derivative classification. Source: E.O. 13526, section 6.1(o).

Digital Asset: The digital content owned by an individual or organization. Digital assets are any digital material owned by an enterprise or individual including text, graphics, audio, video, and animations. Digital content includes individual files such as images, photos, videos, and text files, and also other digital content, such as data in a database. Today, enterprises have a huge amount of digital assets that require managing. PC Magazine, (*http://www.pcmag.com/encyclopedia_term/0,1237,t=digital+asset&i=41283,00.asp*) Copyright © 1981–2012, The Computer Language Company, Inc.

Equity: Information that was originated, created by, classified by, or concerns the activities of another government agency or organization and only they can declassify it. Records that contain other agency "equities" must be referred to those agencies for declassification review. Sources: 32 C.F.R. Parts 2001 and 2003 Classified National Security Information; Final Rule, section 2001. 92(g), 75 FR 37279, Document Number 2010-15443 and The U.S. Department of Justice, Office of Information and Privacy (*http://www.justice.gov/open/declassification-faq.html*).

Executive Order (E.O.) 13526: E.O. 13526, "Classified National Security Information," signed by President Barack Obama in 2008. This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Its immediate predecessor Orders were E.O. 12958, signed by President William J. Clinton in 1995, and E.O. 13292, which amended E.O. 12958, and was signed by President George W. Bush in 2003. E.O. 12958 established the concept of automatic declassification, in which all classified records shall be automatically declassified on December 31 of the year that is 25 years from the date of their original creation, unless properly exempted from declassification. E.O. 13292 and E.O. 13526 continued this automatic declassification requirement. Source: E.O. 13526, introduction and section 3.3(a).

Foreign Relations of the United States (FRUS): The official documentary historical record of major U.S. foreign policy decisions and significant diplomatic activity. The series, which is produced by the State Department's Office of the Historian, began in 1861 and now comprises more than 350 individual volumes. The volumes published since 1980 increasingly contain declassified records from all the foreign affairs agencies. Source: The U.S. Department of State, Office of the Historian, (*www.state.gov/r/pa/ho/frus/*).

Formerly Restricted Data (FRD) Information: As designated by the Department of Energy under provisions of the Atomic Energy Act, FRD information is classified information that has been removed from the Restricted Data category after the Departments of Energy and Defense jointly determine that it relates primarily to the military utilization of atomic weapons and can be adequately safeguarded in a manner *similar* to national security information. FRD information is automatically excluded from declassification review under the current Executive Order. Sources: Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq.: section 142 and 10 C.F.R. PART 1045 Nuclear Classification and Declassification; Final Rule, section 1045.3.

Historically Significant Records: Federal records, Presidential papers, or Presidential records that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code. Records or materials that demonstrate and record the national security policies, actions, and decisions of the United States, including (1) policies, events, actions, and decisions that led to significant national security outcomes; and (2) the development and evolution of significant United States national security policies, actions, and decisions. These records will provide a significantly different perspective in general from records and materials publicly available in other historical sources and would need to be addressed through ad hoc record searches outside any systematic declassification program established under Executive order. Sources: E.O. 13526, section 6.1(ii) and the Public Interest Declassification Board enabling legislation: Public Law 106-657, section 709.

Index: The process of creating an ordered list of concepts, expressed as terms or phrases, with pointers to the place in indexed material where those concepts appear.

Source: *A Glossary of Archival and Records Terminology,* Copyright © 2012, Society of American Archivists, (*http://www2.archivists.org/glossary*). At the National Archives, indexing occurs during archival processing and entails documenting decisions to remove certain records from public access. Typically, records are restricted from public access for statutory reasons (e.g. the Privacy Act) or for reasons of national security.

Information Security Oversight Office (ISOO): A component of the National Archives that receives program and policy guidance from the National Security Staff at the White House. Among its main responsibilities, ISOO oversees the security classification programs in both Government and industry and reports annually to the President on their status. Source: ISOO Report to the President, FY 2011.

Kyl-Lott Amendment: This provision is named after its two legislative sponsors, Senators Trent Lott and John Kyl, who authored an amendment to the National Defense Authorization Act of 1999. Section 3161, "Protection against Inadvertent Release of Restricted Data and Formerly Restricted Data," requires the Department of Energy to develop a plan to prevent the release of nuclear weapons design and employment information. Among its provisions is the requirement that records subject to the automatic declassification provisions of E.O. 13526 be reviewed on a page-by-page basis for Restricted Data and Formerly Restricted Data unless the originating agency certifies that the records are highly unlikely to contain RD or FRD information. Source: Public Law 105-261, section 3161.

Mandatory Declassification Review: The review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of Executive Order 13526. Source: E.O. 13526, section 6.1(aa).

Metadata: A characterization or description documenting the identification, management, nature, use, or location of information resources (data). Source: *A Glossary of Archival and Records Terminology* Copyright, © 2012, Society of American Archivists, (*http://www2.archivists.org/glossary*).

Multiple Agency Equities: Refers to when a record contains information that was originated, classified by, or concerns the activities of *more than one* government agency or organization. These records are challenging to review for public access as they must be referred to each agency that owns information in the record. Source: E.O. 13526, section 3.3 (b) (3).

National Declassification Center: The center established within the National Archives to streamline declassification processes, facilitate quality-assurance measures, and implement standardized training regarding the declassification of records determined to have permanent historical value. E.O. 13526, section 3.7.

National Security: The national defense or foreign relations of the United States. Source: E.O. 13526, section 6.1(cc).

Original Classification: The initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure. Source: E.O. 13526, section 6.1(ff).

Petabyte: 1,024 terabytes or 1,125,899,906,842,624 bytes. See "Byte; Terabyte." Source: "Petabyte." Dictionary.com Unabridged. Random House, Inc. 21 Nov. 2012.

Predictive Analytics: An area of statistical analysis that deals with extracting information from data and using it to predict future trends and behavior patterns. The core of predictive analytics relies on capturing relationships between explanatory variables and the predicted variables from past occurrences, and exploiting it to predict future outcomes. It is important to note, however, that the accuracy and usability of results will depend greatly on the level of data analysis and the quality of assumptions. Source: Nyce, Charles (2007), Predictive Analytics White Paper, American Institute for Chartered Property Casualty Underwriters/Insurance Institute of America, p. 1.

Records Having Permanent Historical Value: Federal records, Presidential papers, or Presidential records that the Archivist has determined should be maintained permanently in accordance with title 44, United States Code. Source: E.O. 13526, section 6.1(ii).

Referral of Records: The act of identifying and sourcing information to the original information owner and requesting review of that information for declassification or other access measure. The process of referring records entails the identification of records containing classified information that originated with other agencies or the disclosure of which would affect the interests or activities of other agencies. Those records that could reasonably be expected to fall under one or more of the exemptions in section 3.3(b) of the Order are eligible for referral. The referral process also entails formal notification to those agencies, making the records available for review by those agencies, and recording final agency determinations. Sources: E.O. 13526, section 3.3(d)(3) and 32 C.F.R. Parts 2001 and 2003 Classified National Security Information; Final Rule, section 2001.34.

Records: The records of an agency and Presidential papers or Presidential records, as those terms are defined in title 44, United States Code, including those created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the contract, license, certificate, or grant. Source: E.O. 13526, section 6.1(hh).

Restricted Data (RD) Information: Information concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; and the use of special nuclear material to *generate* electricity. RD information is automatically excluded from declassification review under the current Executive Order. Sources: Public Law 83-703 The Atomic Energy Act of 1954, 42 U.S.C. § 2011 et seq.: section 11 and 10 C.F.R. PART 1045 Nuclear Classification and Declassification; Final Rule, section 1045.3.

Schedule: The process of identifying and describing records held by an organization, determining their retention period, and describing disposition actions throughout their life cycle. Source: *A Glossary of Archival and Records Terminology,* Copyright © 2012, Society of American Archivists, (*http://www2.archivists.org/glossary*).

Systematic Declassification Review: The review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code. Systematic Declassification Review occurs to those records containing information exempted from automatic declassification. This includes individual records as well as file series of records. Agencies shall prioritize their review of such records in accordance with priorities established by the NDC. Sources: E.O. 13526, section 6.1(pp) and 32 C.F.R. Parts 2001 and 2003 Classified National Security Information; Final Rule, section 2001.31.

Terabyte: 1024 gigabytes or 1,099,511,627,776 bytes; also: one trillion bytes. See "Byte; Petabyte." Source: "Terabyte." Merriam-Webster.com. Merriam-Webster, 2011.

Transfer: The process of moving records as part of their scheduled disposition, especially from an office to a records center, or from a records center to an archives. Source: *A Glossary of Archival and Records Terminology,* Copyright © 2012, Society of American Archivists, (*http://www2.archivists.org/glossary*).

APPENDIX D

BOARD'S AUTHORIZING STATUTE

SEC. 701. SHORT TITLE.

This title may be cited as the "Public Interest Declassification Act of 2000".

SEC. 702. FINDINGS.

Congress makes the following findings:

(1) It is in the national interest to establish an effective, coordinated, and cost-effective means by which records on specific subjects of extraordinary public interest that do not undermine the national security interests of the United States may be collected, retained, reviewed, and disseminated to Congress, policymakers in the executive branch, and the public.

(2) Ensuring, through such measures, public access to information that does not require continued protection to maintain the national security interests of the United States is a key to striking the balance between secrecy essential to national security and the openness that is central to the proper functioning of the political institutions of the United States.

SEC. 703. PUBLIC INTEREST DECLASSIFICATION BOARD.

(a) ESTABLISHMENT.—

(1) There is established within the executive branch of the United States a board to be known as the "Public Interest Declassification Board" (in this title referred to as the "Board").

(2) The Board shall report directly to the President or, upon designation by the President, the Vice President, the Attorney General, or other designee of the President. The other designee of the President under this paragraph may not be an agency head or official authorized to classify information under Executive Order 12958, or any successor order.

(b)PURPOSES.—The purposes of the Board are as follows:

(1) To advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on the systematic, thorough, coordinated, and comprehensive identification, collection, review for declassification, and release to Congress, interested agencies, and the public of declassified records and materials (including donated historical materials) that are of archival value, including records and materials of extraordinary public interest.

(2) To promote the fullest possible public access to a thorough, accurate, and reliable documentary record of significant United States national security decisions and significant United States national security activities in order to—

(A) support the oversight and legislative functions of Congress;

(B) support the policymaking role of the executive branch;

(C) respond to the interest of the public in national security matters; and

(D) promote reliable historical analysis and new avenues of historical study in national security matters.

(3) To provide recommendations to the President for the identification, collection, and review for declassification of information of extraordinary public interest that does not undermine the national security of the United States, to be undertaken in accordance with a declassification program that has been established or may be established by the President by Executive order.

(4) To advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on policies deriving from the issuance by the President of Executive orders regarding the classification and declassification of national security information.

(5) To review and make recommendations to the President in a timely manner with respect to any congressional request, made by the committee of jurisdiction, to declassify certain records or to reconsider a declination to declassify specific records.

(c) MEMBERSHIP.—

(1) The Board shall be composed of nine individuals appointed from among citizens of the United States who are preeminent in the fields of history, national security, foreign policy, intelligence policy, social science, law, or See: Public Law 106-567 (December 27, 2000), as amended by section 1102 of P.L. 108-458 (Intelligence Reform and Terrorism Prevention Act of 2004) (December 17, 2004), and as further amended by section 602 of P.L. 110-53 (Implementing Recommendations of the 9/11 Commission Act of 2007) (August 3, 2007).

TITLE VII—DECLASSIFICATION OF INFORMATION
41
APPENDIX D
archives, including individuals who have served in Congress or otherwise in the Federal Government or have otherwise engaged in research, scholarship, or publication in such fields on matters relating to the national security of the United States, of whom—
(A) five shall be appointed by the President;
(B) one shall be appointed by the Speaker of the House of Representatives;
(C) one shall be appointed by the majority leader of the Senate;
(D) one shall be appointed by the minority leader of the Senate; and
(E) one shall be appointed by the minority leader of the House of Representatives.
(2) (A) Of the members initially appointed to the Board by the President—
(i) three shall be appointed for a term of 4 years;
(ii) one shall be appointed for a term of 3 years; and
(iii) one shall be appointed for a term of 2 years.
(B) The members initially appointed to the Board by the Speaker of the House of Representatives or by the majority leader of the Senate shall be appointed for a term of 3 years.
(C) The members initially appointed to the Board by the minority leader of the House of Representatives or the Senate shall be appointed for a term of 2 years.
(D) Any subsequent appointment to the Board shall be for a term of 3 years.
(3) A vacancy in the Board shall be filled in the same manner as the original appointment. A member of the Board appointed to fill a vacancy before the expiration of a term shall serve for the remainder of the term.
(4) A member of the Board may be appointed to a new term on the Board upon the expiration of the member's term on the Board, except that no member may serve more than three full terms on the Board.
(d) CHAIRPERSON; EXECUTIVE SECRETARY.—
(1) (A) The President shall designate one of the members of the Board as the chairperson of the Board.
(B) The term of service as Chairperson of the Board shall be 2 years.
(C) A member serving as Chairperson of the Board may be redesignated as Chairperson of the Board upon the expiration of the member's term as Chairperson of the Board, except that no member shall serve as Chairperson of the Board for more than 6 years.
(2) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Board.
(e) MEETINGS.—The Board shall meet as needed to accomplish its mission, consistent with the availability of funds. A majority of the members of the Board shall constitute a quorum.
(f) STAFF.—Any employee of the Federal Government may be detailed to the Board, with the agreement of and without reimbursement to the detailing agency, and such detail shall be without interruption or loss of civil, military, or foreign service status or privilege.
(g) SECURITY. —
(1) The members and staff of the Board shall, as a condition of appointment to or employment with the Board, hold appropriate security clearances for access to the classified records and materials to be reviewed by the Board or its staff, and shall follow the guidance and practices on security under applicable Executive orders and Presidential or agency directives.
(2) The head of an agency shall, as a condition of granting access to a member of the Board, the Executive Secretary of the Board, or a member of the staff of the Board to classified records or materials of the agency under this title, require the member, the Executive Secretary, or the member of the staff, as the case may be, to—
(A) execute an agreement regarding the security of such records or materials that is approved by the head of the . agency; and
(B) hold an appropriate security clearance granted or recognized under the standard procedures and eligibility criteria of the agency, including any special access approval required for access to such records or materials.
(3) The members of the Board, the Executive Secretary of the Board, and the members of the staff of the Board may not use any information acquired in the course of their official activities on the Board for nonofficial purposes.
(4) For purposes of any law or regulation governing access to classified information that pertains to the national security of the United States, and subject to any limitations on access arising under section 706(b), and to facilitate the advisory functions of the Board under this title, a member of the Board seeking access to a record or material under this title shall be deemed for purposes of

this subsection to have a need to know the contents of the record or material.

(h) COMPENSATION. —

(1) Each member of the Board shall receive compensation at a rate not to exceed the daily equivalent of the annual rate of basic pay payable for positions at ES–1 of the Senior Executive Service under section 5382 of title 5, United States Code, for each day such member is engaged in the actual performance of duties of the Board. 42

(2) Members of the Board shall be allowed travel expenses, including per diem in lieu of subsistence at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of the duties of the Board.

(i) GUIDANCE; ANNUAL BUDGET. —

(1) On behalf of the President, the Assistant to the President for National Security Affairs shall provide guidance on policy to the Board.

(2) The Executive Secretary of the Board, under the direction of the Chairperson of the Board and the Board, and acting in consultation with the Archivist of the United States, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget, shall prepare the annual budget of the Board.

(j) SUPPORT.—The Information Security Oversight Office may support the activities of the Board under this title. Such support shall be provided on a reimbursable basis.

(k) PUBLIC AVAILABILITY OF RECORDS AND REPORTS. —

(1) The Board shall make available for public inspection records of its proceedings and reports prepared in the course of its activities under this title to the extent such records and reports are not classified and would not be exempt from release under the provisions of section 552 of title 5, United States Code.

(2) In making records and reports available under paragraph (1), the Board shall coordinate the release of such records and reports with appropriate officials from agencies with expertise in classified information in order to ensure that such records and reports do not inadvertently contain classified information.

(l) APPLICABILITY OF CERTAIN ADMINISTRATIVE LAWS.—The provisions of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the activities of the Board under this title. However, the records of the Board shall be governed by the provisions of the Federal Records Act of 1950.

SEC. 704. IDENTIFICATION, COLLECTION, AND REVIEW FOR DECLASSIFICATION OF INFORMATION OF ARCHIVAL VALUE OR EXTRAORDINARY PUBLIC INTEREST.

(a) BRIEFINGS ON AGENCY DECLASSIFICATION PROGRAMS. —

(1) As requested by the Board, or by the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives, the head of any agency with the authority under an Executive order to classify information shall provide to the Board, the Select Committee on Intelligence of the Senate, or the Permanent Select Committee on Intelligence of the House of Representatives, on an annual basis, a summary briefing and report on such agency's progress and plans in the declassification of national security information. Such briefing shall cover the declassification goals set by statute, regulation, or policy, the agency's progress with respect to such goals, and the agency's planned goals and priorities for its declassification activities over the next 2 fiscal years. Agency briefings and reports shall give particular attention to progress on the declassification of records and materials that are of archival value or extraordinary public interest to the people of the United States.

(2)(A) The annual briefing and report under paragraph (1) for agencies within the Department of Defense, including the military departments and the elements of the intelligence community, shall be provided on a consolidated basis.

(B) In this paragraph, the term "elements of the intelligence community" means the elements of the intelligence community specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(b) RECOMMENDATIONS ON AGENCY DECLASSIFICATION PROGRAMS. —

(1) Upon reviewing and discussing declassification plans and progress with an agency, the Board shall provide to the head of the agency the written recommendations of the Board as to how the agency's declassification program could be improved. A copy of each recommendation shall also be submitted to the Assistant to the President for National Security Affairs and the Director of the Office of

Management and Budget.
(2) Consistent with the provisions of section 703(k), the Board's recommendations to the head of an agency under paragraph (1) shall become public 60 days after such recommendations are sent to the head of the agency under that paragraph.
(c) RECOMMENDATIONS ON SPECIAL SEARCHES FOR RECORDS OF EXTRAORDINARY PUBLIC INTEREST. —
(1) The Board shall also make recommendations to the President regarding proposed initiatives to identify, collect, and review for declassification classified records and materials of extraordinary public interest.
(2) In making recommendations under paragraph (1), the Board shall consider the following:
(A) The opinions and requests of Members of Congress, including opinions and requests expressed or embodied in letters or legislative proposals, and also including specific requests for the declassification of certain records or for the reconsideration of declinations to declassify specific records.
(B) The opinions and requests of the National Security Council, the Director of Central Intelligence, and the heads of other agencies.
43
(C) The opinions of United States citizens.
(D) The opinions of members of the Board.
(E) The impact of special searches on systematic and all other on-going declassification programs.
(F) The costs (including budgetary costs) and the impact that complying with the recommendations would have on agency budgets, programs, and operations.
(G) The benefits of the recommendations.
(H) The impact of compliance with the recommendations on the national security of the United States.
(d) PRESIDENT'S DECLASSIFICATION PRIORITIES.—
(1) Concurrent with the submission to Congress of the budget of the President each fiscal year under section 1105 of title 31, United States Code, the Director of the Office of Management and Budget shall publish a description of the President's declassification program and priorities, together with a listing of the funds requested to implement that program.
(2) Nothing in this title shall be construed to substitute or supersede, or establish a funding process for, any declassification program that has been established or may be established by the President by Executive order.
(e) DECLASSIFICATION REVIEWS. —
(1) IN GENERAL—If requested by the President, the Board shall review in a timely manner certain records or declinations to declassify specific records, the declassification of which has been the subject of specific congressional request described in section 703(b)(5).
(2) AUTHORITY OF THE BOARD—Upon receiving a congressional request described in section 703(b)(5), the Board may conduct the review and make the recommendations described in that section, regardless of whether such a review is requested by the President.
(3) REPORTING—Any recommendations submitted to the President by the Board under section 703(b)(5), shall be submitted to the chairman and ranking member of the committee of Congress that made the request relating to such recommendations.
SEC. 705. PROTECTION OF NATIONAL SECURITY INFORMATION AND OTHER INFORMATION.
(a) IN GENERAL.—Nothing in this title shall be construed to limit the authority of the head of an agency to classify information or to continue the classification of information previously classified by that agency.
(b) SPECIAL ACCESS PROGRAMS.—Nothing in this title shall be construed to limit the authority of the head of an agency to grant or deny access to a special access program.
(c) AUTHORITIES OF DIRECTOR OF CENTRAL INTELLIGENCE.—Nothing in this title shall be construed to limit the authorities of the Director of Central Intelligence as the head of the intelligence community, including the Director's responsibility to protect intelligence sources and methods from unauthorized disclosure as required by section 103(c)(6) of the National Security Act of 1947 (50 U.S.C. 403– 3(c)(6)).
(d) EXEMPTIONS TO RELEASE OF INFORMATION.—Nothing in this title shall be construed to limit any exemption or exception to the release to the public under this title of information that is protected under subsection (b) of section 552 of title 5, United States Code (commonly referred to as the "Freedom of Information Act"), or section 552a of title 5, United States Code (commonly referred to as the "Privacy Act").
(e) WITHHOLDING INFORMATION FROM CONGRESS.—Nothing in this title shall be construed to authorize the withholding of information from Congress.

SEC. 706. STANDARDS AND PROCEDURES.

(a) LIAISON.—(1) The head of each agency with the authority under an Executive order to classify information and the head of each Federal Presidential library shall designate an employee of such agency or library to act as liaison to the Board for purposes of this title.

(2) The Board may establish liaison and otherwise consult with such other historical and advisory committees as the Board considers appropriate for purposes of this title.

(b) LIMITATIONS ON ACCESS. —

(1) (A) Except as provided in paragraph (2), if the head of an agency or the head of a Federal Presidential library determines it necessary to deny or restrict access of the Board, or of the agency or library liaison to the Board, to information contained in a record or material, in whole or in part, the head of the agency or the head of the library shall promptly notify the Board in writing of such determination.

(B) Each notice to the Board under subparagraph (A) shall include a description of the nature of the records or materials, and a justification for the determination, covered by such notice.

44

(2) In the case of a determination referred to in paragraph (1) with respect to a special access program created by the Secretary of Defense, the Director of Central Intelligence, or the head of any other agency, the notification of denial of access under paragraph (1), including a description of the nature of the Board's request for access, shall be submitted to the Assistant to the President for National Security Affairs rather than to the Board.

(c) DISCRETION TO DISCLOSE.—At the conclusion of a declassification review, the head of an agency may, in the discretion of the head of the agency, determine that the public's interest in the disclosure of records or materials of the agency covered by such review, and still properly classified, outweighs the Government's need to protect such records or materials, and may release such records or materials in accordance with the provisions of Executive Order No. 12958 or any successor order to such Executive order.

(d) DISCRETION TO PROTECT.—At the conclusion of a declassification review, the head of an agency may, in the discretion of the head of the agency, determine that the interest of the agency in the protection of records or materials of the agency covered by such review, and still properly classified, outweighs the public's need for access to such records or materials, and may deny release of such records or materials in accordance with the provisions of Executive Order No. 12958 or any successor order to such Executive order.

(e) REPORTS. —

(1) (A) Except as provided in paragraph (2), the Board shall annually submit to the appropriate congressional committees a report on the activities of the Board under this title, including summary information regarding any denials to the Board by the head of an agency or the head of a Federal Presidential library of access to records or materials under this title.

(B) In this paragraph, the term "appropriate congressional committees" means the Select Committee on Intelligence and the Committee on Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Government Reform of the House of Representatives.

(2) Notwithstanding paragraph (1), notice that the Board has been denied access to records and materials, and a justification for the determination in support of the denial, shall be submitted by the agency denying the access as follows:

(A) In the case of the denial of access to a special access program created by the Secretary of Defense, to the Committees on Armed Services and Appropriations of the Senate and to the Committees on Armed Services and Appropriations of the House of Representatives.

(B) In the case of the denial of access to a special access program created by the Director of Central Intelligence, or by the head of any other agency (including the Department of Defense) if the special access program pertains to intelligence activities, or of access to any information and materials relating to intelligence sources and methods, to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

(C) In the case of the denial of access to a special access program created by the Secretary of Energy or the Administrator for Nuclear Security, to the Committees on Armed Services and Appropriations and the Select Committee on Intelligence of the Senate and to the Committees on Armed Services and Appropriations and the Permanent Select Committee on Intelligence of the House of Representatives.

(f) NOTIFICATION OF REVIEW.—In response to a

specific congressional request for declassification review described in section 703(b)(5), the Board shall advise the originators of the request in a timely manner whether the Board intends to conduct such review.

SEC. 707. JUDICIAL REVIEW.

Nothing in this title limits the protection afforded to any information under any other provision of law. This title is not intended and may not be construed to create any right or benefit, substantive or procedural, enforceable against the United States, its agencies, its officers, or its employees. This title does not modify in any way the substantive criteria or procedures for the classification of information, nor does this title create any right or benefit subject to judicial review.

SEC. 708. FUNDING.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is hereby authorized to be appropriated to carry out the provisions of this title amounts as follows:

(1) For fiscal year 2001, $650,000.

(2) For each fiscal year after fiscal year 2001, such sums as may be necessary for such fiscal year.

(b) FUNDING REQUESTS.—The President shall include in the budget submitted to Congress for each fiscal year under section 1105 of title 31, United States Code, a request for amounts for the activities of the Board under this title during such fiscal year.

SEC. 709. DEFINITIONS.

In this title:

(1) AGENCY.—

(A) Except as provided in subparagraph (B), the term "agency" means the following:

(i) An Executive agency, as that term is defined in section 105 of title 5, United States Code.

(ii) A military department, as that term is defined in section 102 of such title.

45

(iii) Any other entity in the executive branch that comes into the possession of classified information.

(B) The term does not include the Board.

(2) CLASSIFIED MATERIAL OR RECORD.— The terms "classified material" and "classified record" include any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work,

photograph, film, microfilm, sound recording, videotape, machine readable records, and other documentary material, regardless of physical form or characteristics, that has been determined pursuant to Executive order to require protection against unauthorized disclosure in the interests of the national security of the United States.

(3) DECLASSIFICATION.—The term "declassification" means the process by which records or materials that have been classified are determined no longer to require protection from unauthorized disclosure to protect the national security of the United States.

(4) DONATED HISTORICAL MATERIAL.—The term "donated historical material" means collections of personal papers donated or given to a Federal Presidential library or other archival repository under a deed of gift or otherwise.

(5) FEDERAL PRESIDENTIAL LIBRARY.—The term "Federal Presidential library" means a library operated and maintained by the United States Government through the National Archives and Records Administration under the applicable provisions of the Federal Records Act of 1950.

(6) NATIONAL SECURITY.—The term "national security" means the national defense or foreign relations of the United States.

(7) RECORDS OR MATERIALS OF EXTRAORDINARY PUBLIC INTEREST.—The term "records or materials of extraordinary public interest" means records or materials that—

(A) demonstrate and record the national security policies, actions, and decisions of the United States, including—

(i) policies, events, actions, and decisions which led to significant national security outcomes; and

(ii) the development and evolution of significant United States national security policies, actions, and decisions;

(B) will provide a significantly different perspective in general from records and materials publicly available in other historical sources; and

(C) would need to be addressed through ad hoc record searches outside any systematic declassification program established under Executive order.

(8) RECORDS OF ARCHIVAL VALUE.—The term "records of archival value" means records that have been determined by the Archivist of the United States to have sufficient historical or other value to warrant their continued preservation by the Federal Government.

SEC. 710. EFFECTIVE DATE; SUNSET.

(a) EFFECTIVE DATE.—This title shall take effect on the date that is 120 days after the date of the enactment of this Act.

(b) SUNSET.—The provisions of this title shall expire on December 31, 2012, unless reauthorized by statute.

"Despite the best of intentions, the classification system, largely unchanged since the Eisenhower administration, has grown out of control. More information is being classified and for extended periods of time. Security rules proliferate, becoming more complex yet remaining unrelated to the threat. Security costs increase as inconsistent requirements are imposed by different agencies or by different program managers within the same agency.

This accretion of security rules and requirements to protect classified information does not make the system work better. Indeed, the classification system is not trusted on the inside any more than it is on the outside. Insiders do not trust it to protect information that needs protection. Outsiders do not trust it to release information that does not need protection.

This Cold War classification system can be simplified."

Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994, Joint Security Commission

SECURITY CLASSIFICATION (If any)

3354

DISPOSITION FORM

FILE NO.	SUBJECT
	Presidential Order Affecting Security Classification

TO	FROM	DATE	COMMENT NO. 1
See Distribution	AG	20 Nov 53	

Col.Geo.E.Campbell/60235/lm

1. By Executive Order 10501, dated 6 November 1953, the President has eliminated the use of "RESTRICTED" classification, and the "SECURITY INFORMATION" notation. This order is to become effective 15 December 1953. Definitions of the remaining categories of classification are as follows:

a. TOP SECRET: Except as may be expressly provided by statute, the use of the classification TOP SECRET shall be authorized, by appropriate authority, only for defense information or material which requires the highest degree of protection. The TOP SECRET classification shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.

b. SECRET: Except as may be expressly provided by statute, the use of the classification SECRET shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations.

c. CONFIDENTIAL: Except as may be expressly provided by statute, the use of the classification CONFIDENTIAL shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the nation.

2. All Agency matter now classified "RESTRICTED" (except that noted in paragraph 3 below) will be automatically declassified 15 December 1953. Material originated by this Agency, now outstanding, bearing the classification of "RESTRICTED", may be upgraded to "CONFIDENTIAL" provided it meets the standard set forth in paragraph 1c. There will be no mass upgrading of "RESTRICTED" material to "CONFIDENTIAL". A document can only be upgraded by its originator, and only on the basis of its content.

3. Exceptions to this Executive Order are as follows:

a. CRYPTOGRAPHIC SECURITY. In order to preserve and maintain cryptographic security as required by the Act of 13 May 1950 (Public Law, 513, 81st Congress):

PUBLIC INTEREST
DECLASSIFICATION BOARD
c/o Information Security Oversight Office
700 Pennsylvania Avenue, NW
Room 503
Washington D.C. 20408

Telephone: 202.357.5250
Fax: 202.357.5907
pidb@nara.gov

www.archives.gov/declassification/pidb